Silicon Flatirons

A Center for Law, Technology, and Entrepreneurship at the University of Colorado

Silicon Flatirons Roundtable Series:
THE FUTURE OF THE INTERNET OF THINGS IN MISSION CRITICAL APPLICATIONS

Wednesday, June 22, 2016, 3:00 PM - 6:00 PM
Hosted by Kelley Drye & Warren LLP

The Internet of Things (IoT), as the ecosystem of IP networked applications, services, and devices is called, promises both to benefit consumers and to raise challenging issues for policymakers. One under-appreciated issue of major significance is that mission critical applications—e.g., public safety, health care, and transportation—sometimes do not take particular care to ensure that they are developed with an eye towards secure, sustainable, and reliable functioning. In the health care environment, for example, new devices and applications may be built for efficiency, not security, and may use unlicensed wireless networks or devices that are vulnerable to interference or jamming. Media reports have also highlighted potential risks in the transportation space, including remote hacking of unmanned aerial systems and connected cars.

The governance challenge for IoT systems is that there is often a lack of trust among actors in the ecosystem; limited incentives for developers to build sustainable, secure, privacy-protective, and maintainable systems; a lack of technical expertise in addressing the unique oversight challenges posed by software and Internet technology; and a coordination challenge among the range of actors in this space. Government policy can help the industry address these concerns, but the relevant expertise and authority to address these issues is dispersed broadly across the government, and the new institutional models for oversight in this area are only being developed. At this roundtable, we will bring together a group of leading researchers, government policymakers, industry leaders, and consumer advocates to discuss the security and performance challenges related to the use of Internet of Things technologies in mission critical environments.

AGENDA

3:00 – 3:15 **Agenda overview and introductions**
Phil Weiser

3:15 – 4:00 **What are the security concerns involved with mission critical IoT devices and how can we minimize the risk?**
Firestarter: Aneesh Chopra

4:00 – 4:45 **How can government and industry increase the likelihood that mission critical IoT devices operate reliably?**
Firestarter: Dale Hatfield

4:45 – 5:30 **What institutional tools can governmental agencies use to engage in adaptive regulatory oversight in this area? How can governmental agencies best collaborate across sectors as Internet of Things technologies touch on a range of areas from health care to transportation?**
Firestarter: Ellen Goodman

5:30 – 6:00 **Wrap Up**

Silicon Flatirons

A Center for Law, Technology, and Entrepreneurship at the University of Colorado

Silicon Flatirons Roundtable Series:
THE FUTURE OF THE INTERNET OF THINGS IN MISSION CRITICAL APPLICATIONS

Wednesday, June 22, 2016, 3:00 PM - 6:00 PM
Hosted by Kelley Drye & Warren LLP

Background Sources

The following readings include material not intended for distribution.

Gary Matuszak et.al., *Security and the IoT Ecosystem* (KPMG International, 2015), *available at* https://www.kpmg.com/CO/es/IssuesAndInsights/ArticlesPublications/Documents/Security%20and%20the%20IoT%20Ecosystem.pdf.

Bruce Schneier, *The Internet of Things is Wildly Insecure – And Often Unpatchable*, Wired (Jan. 6, 2014), *available at* http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

FTC Staff Report, *Internet of Things, Privacy and Security in a Connected World* (Jan. 2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Mingyi Zhao et al., *An Empirical Study of Web Vulnerability Discovery Ecosystems*, 15 CSS 1105 (2015), *available at* https://www.ftc.gov/system/files/documents/public_comments/2015/10/00079-98131.pdf.

Kenneth Corbin, *The Internet of Things Brings Far-Reaching Security Threats*, CIO (Aug. 8, 2014), *available at* http://www.cio.com/article/2462407/mobile-security/the-internet-of-things-brings-far-reaching-security-threats.html.

IoT Devices Easily Hacked to be Backdoors: Experiment, SecurityWeek News (Jan. 13, 2016), *available at* http://www.securityweek.com/iot,devices4easily-hacked-be-backdoors-experiment.

Jordan Gass-Poore, *Researchers Hope This Invention Could Wave Away Medical Data Hacks*, NPR (May 10, 2016), *available at* http://www.npr.org/sections/alltechconsidered/2016/05/10/476941159/researchers-hope-this-invention-could-wave-away-medical-data-hacks.

Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85 (2014), *available at* http://www.texaslrev.com/wp-content/uploads/2015/08/Peppet-93-1.pdf.

Milan Goldas, *Connectivity That Will Shape the Future of Mission Critical IoT Applications*, IoTNow (July 06, 2015), *available at* http://www.iot-now.com/2015/07/06/34522-connectivity-that-will-shape-the-future-of-mission-critical-iot-applications/.

Notice, Request for Public Comment, *The Benefits, Challenges, and Potential Roles for Government in Fostering the Advancement of the Internet of Things*, 81 Fed. Reg. 19956 (published April 06, 2016), *available at* https://www.federalregister.gov/articles/2016/04/06/2016-07892/the-benefits-challenges-and-potential-roles-for-the-government-in-fostering-the-advancement-of-the.

Daniel Castro & Joshua New, *10 Policy Principles for Unlocking the Potential of the Internet of Things*, (Center for Data Innovation, 2014), *available at* http://www2.datainnovation.org/2014-iot-policy-principles.pdf.

Dana Blouin, *Unique Public-Private Partnership Targets IoT Security*, CMSWire.com (Aug. 31, 2015), *available at* http://www.cmswire.com/internet-of-things/unique-public-private-partnership-targets-iot-security/.

Mari C. Domingo, *An Overview of the Internet of Things for People with Disabilities*, 35 J. of Network and Computer Applications 584 (2011), *available at* http://ac.els-cdn.com/S1084804511002025/1-s2.0-S1084804511002025-main.pdf?_tid=314be77c-2355-11e6-a077-00000aacb362&acdnat=1464276129_77d248e6a7d29c358ce014784520a528.

Joshua New & Daniel Castro, *Why Countries Need National Strategies for the Internet of Things* (Center for Data Innovation, 2015), *available at* http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

Silicon Flatirons

A Center for Law, Technology, and Entrepreneurship at the University of Colorado

Silicon Flatirons Roundtable Series:
THE FUTURE OF THE INTERNET OF THINGS IN MISSION CRITICAL APPLICATIONS

Wednesday, June 22, 2016, 3:00 PM - 6:00 PM
Hosted by Kelley Drye & Warren LLP

PARTICIPANTS

Rebecca Arbogast, Senior Vice President, Global Public Policy, Comcast Corporation
Jon Banks, Senior Vice President, Law and Policy, USTelecom Association
Jack Belcher, Chief Information Officer, Department of Technology Services, Arlington County, Virginia
Jeff Blattner, President, Legal Policy Solutions, PLLC
Len Cali, Senior Vice President, Global Public Policy, AT&T
Aneesh Chopra, Co-Founder and Executive Vice President, Hunch Analytics
Ryan Clough, General Counsel, Public Knowledge
Hap Connors, Member, Commonwealth Transportation Board
Christine DeLorme, Attorney Advisor, Office of Commissioner Terrell McSweeny, Federal Trade Commission
Jameson Dempsey, Associate, Kelley Drye & Warren LLP
Scott Deutchman, Deputy General Counsel and Vice President for Legal and External Affairs, NeuStar Inc.
Donna Epps, Vice President Public Policy and Strategic Alliances, Verizon
Michele Farquhar, Partner, Hogan Lovells US LLP
Derik Goatson, Student, University of Colorado Law School
Ellen Goodman, Professor, Rutgers Law School
Joseph Lorenzo Hall, Chief Technologist, The Center for Democracy & Technology
Dale Hatfield, Senior Fellow, Silicon Flatirons
John Heitmann, Partner, Kelley Drye & Warren LLP
Hank Kelly, Partner, Kelley Drye & Warren LLP
Robert Kelly, Partner, Squire Patton Boggs
Linda Kinney, Senior Advisor, Internet Policy, National Telecommunications and Information Administration
Fernando Laguarda, Vice President, External Affairs and Policy Counselor, Time Warner Cable
Jason Livingood, Vice President, Internet Services, Comcast
Christin McMeley, Partner and Chair, Privacy & Security Practice, Davis Wright Tremaine LLP
Blake Reid, Assistant Clinical Professor, University of Colorado Law School
Alex Reynolds, Director, Regulator Affairs, Consumer Technology Association
Glenn Reynolds, Chief of Staff, National Telecommunications and Information Administration
Jonathan Sackner-Bernstein, Former Associate Center Director for Technology and Innovation, US Food and Drug Administration
Jon Sallet, General Counsel, Federal Communications Commission
Eric Schneider, Senior Vice President for Policy and Research, The Commonwealth Fund
Sara Schnittgrund, Director of Student Programs, Silicon Flatirons
Steve Sharkey, Vice President, Government Affairs, Engineering and Technology Policy, T-Mobile
Roger Sherman, Principal, Waneta Strategies
Phil Verveer, Senior Counsel to the Chairman, Federal Communications Commission
Phil Weiser, Executive Director, Silicon Flatirons; Dean, University of Colorado Law School
Jeffrey Westling, Student, University of Colorado Law School

Security and the IoT ecosystem

KPMG International

kpmg.com

Foreword

When it comes to the Internet of Things (IoT), you can believe the hype. In fact, IoT will likely be even bigger than most people think. But success in the IoT space will take more than slick applications, connected devices and advanced analytics; it will also require a robust approach to security, privacy and trust.

For the technology sector, the message from businesses and consumers is clear: be innovative, be bold, and be secure.

It seems obvious that IoT will bring massive growth to those tech companies and IoT developers that are able to carve out a dominant position in this expanding market. However, with evolving market maturity and heightened competition has come mounting concern for current and potential IoT users, particularly around security.

Indeed, as this report suggests, tech firms and IoT service providers will need to work quickly, diligently and decisively to deal with concerns related to security (how well controlled is the device and the infrastructure?), privacy (how is data kept confidential?) and trust (how is customer confidence being addressed?) before they turn into problems. Those that fail to do so will have a difficult time growing in this new environment.

We believe that the technology sector must come together with other vertical and horizontal players in the ecosystem to create a unified approach to security and standards that everyone can live by, and grow with. Today's current state of

fragmentation and competition on standards will only result in greater complexity for users and reduced growth for the IoT sector.

This report aims to catalyze the debate and extend the body of knowledge on IoT security. In the following pages, we start to explore the security, privacy and trust challenges influencing the IoT space and delve into some of the opportunities and models emerging in the market today. Based on a recent global survey of 100 IoT 'user organizations' and supported by one-on-one interviews with industry leaders, academic and KPMG's own IoT professionals, this report hones in on IoT security, privacy and trust, providing practical and actionable advice for all players in the emerging ecosystem.

Over the coming year, KPMG International will take a deeper dive into these key issues. Supported by insights from our global network of technology and IoT professionals, we will explore how these key imperatives are being managed across sectors, applications and ecosystems.

Gary Matuszak

Global Chair
Technology, Media & Telecommunications

Greg Bell

Principal and Services Leader, KPMG Cyber
KPMG in the US

Danny Le

Partner
KPMG in the US

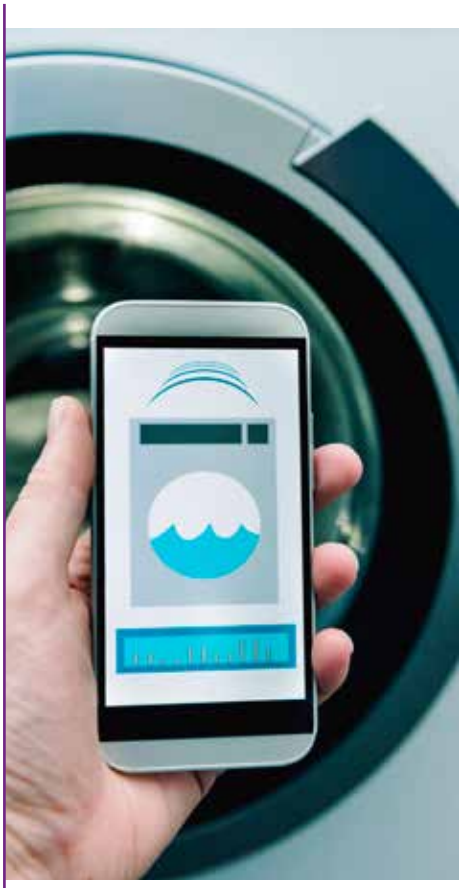
The Internet of Things (IoT)

Combining data, cloud, connectivity, analytics and technology in a way that enables a smart environment in which everyday objects are embedded with network connectivity in order to improve functionality and interaction.

Table of contents

02

Cyber security becomes a ‘must have’



06

Looking for standards

10

Focus on security, privacy and trust

16

Driving security, privacy and trust across the ecosystem

Cyber security becomes a 'must have'

92%

of IoT users are concerned about cyber security

Source: KPMG Cyber Security and IoT Survey

Business leaders may recognize the potential advantages that IoT can offer. But they are also deeply worried about the risks; the majority admit that they don't fully understand the cyber security threats that IoT brings.

But while IoT customers may not be willing to pay extra for security, recent security breaches in consumer data and systems suggest that they will lose confidence and may even avoid solutions providers who fail to take the appropriate measures to protect their security.

Everyone wants to be 'first out the door' with a new IoT solution or product; 89 percent of our survey respondents said they believe that the first movers in IoT will enjoy a clear competitive advantage in their markets. Technology firms and IoT service providers are fighting to get their products out to market faster, eager to capitalize on the massive growth potential of this emerging field.

The rationale is obvious. Those that are able to get to market first and solidify a dominant position in the IoT value chain should be well-placed to parlay their leadership position into rapid and sustainable growth. But the reality is that history is littered with products and ideas that placed speed-to-market over substance and, as such, quickly lost their advantage to other – less nimble but more robust – competitors. Simply put,

companies will need to prioritize security alongside other key considerations such as speed and usability when developing and operating IoT solutions.

This reality is already being borne out. Recent revelations about security vulnerabilities in a number of newer-model automobiles have forced some major manufacturers to conduct massive recalls. Over the summer, the media was abuzz with news of hackers 'hijacking' cars through badly-secured software systems.

Taking the threat seriously

Many organizations are now thinking more clearly about how they might improve IoT security. "At Intel, we believe that integrating security into the platform and into the silicon is critical to helping drive IoT's adoption and scalability. Integrating security at the onset is key to establishing trust for IoT solutions," noted Bridget Karlin, Managing Director, Internet of Things Group Intel. "We've got some great IoT offerings coming onto the market that

> "Our company's understanding of IoT cybersecurity risks is limited, so it has become a top priority."
> – CEO of a European-based IoT user organization

IoT: Rapid growth, massive potential

No one doubts that the Internet of Things (IoT) represents a massive opportunity for businesses, consumers and tech companies. Most organizations are only just starting to scratch the surface of what they can achieve with IoT solutions.

For device manufacturers and application developers, the rapid adoption of IoT-enabled devices is expected to drive a new round of growth and expansion as the number of installed devices sky-rockets. According to IDC Research, the installed base of IoT units will grow 17.5 percent per year. And within the next 5 years, forecasts suggest that the market will be worth a whopping US$7.1 trillion.[1]

However, we believe that as consumers get more and more familiar with the benefits that IoT can deliver – smart appliances, automated vehicles, wearable devices and much more – key concerns around security, privacy and trust are likely to grow.

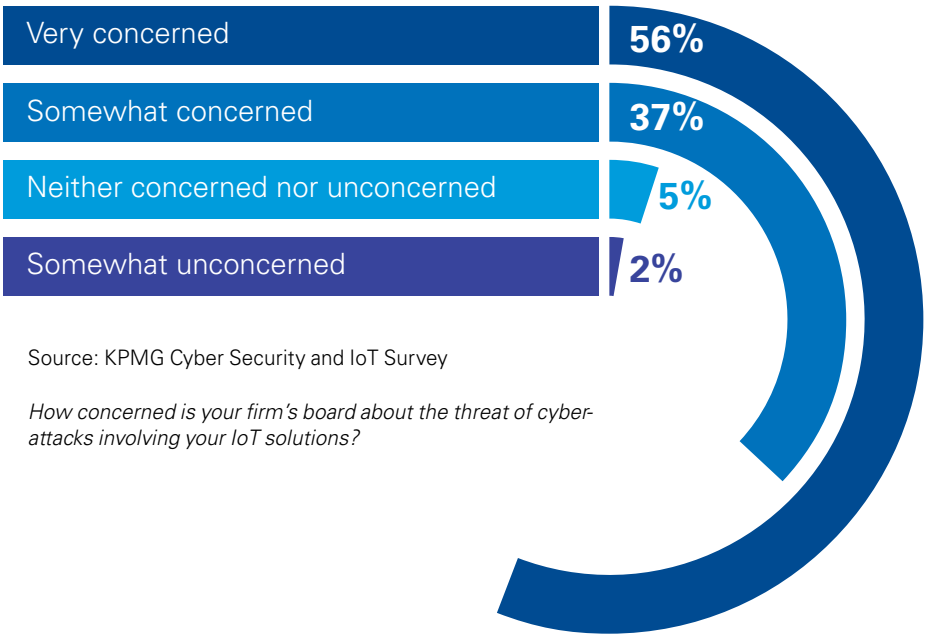
1 Worldwide and Regional Internet of Things 2014–2020 Forecast, IDC Research, 2014

enable secure and scalable end to end IoT solutions using our Intel IoT Platform reference architectures and portfolio of products that provide hardware and software enforced integrity and data privacy."

For their part, IoT users are certainly concerned about the potential impact of a cybersecurity breach within their IoT solutions. More than half – 56 percent – of respondents in our survey said that their board was 'very concerned' about the threat of cyber-attack. More than a third said their board was 'somewhat concerned'.

As one Asia-Pacific-based Chief Risk Officer told us, "Our management board is very concerned about the threats of cyber-attacks, in light of the increasing number of cybercrimes and the vast technologies that are employed for IoT solutions. Naturally, the whole IT system has been designed and integrated with new IoT devices, so any threat can be a significant blockage in our business continuity."

IoT users and their boards are becoming increasingly concerned about the risk of cyber-attack on their IoT solutions



Source: KPMG Cyber Security and IoT Survey

How concerned is your firm's board about the threat of cyber-attacks involving your IoT solutions?

Risks and opportunities

While the 'downside' risk can range from data loss through to denial of service or loss of control of the device, improved security in IoT can also provide significant advantages. Our experience suggests that a strong and robust cyber security stance, commonly accepted standards and strong actions towards earning consumer trust will be key to ensuring long-term advantage and, ultimately, supporting growth.

"Key concepts around IoT security, privacy and trust must be front-and-center for tech firms and IoT solutions developers," noted Danny Le, Partner, KPMG in the US. "The 'upside' to cyber security is coming. In fact, before too long we expect to see organizations turn cyber security prowess into real revenue opportunities by, for example, monetizing identity and usage patterns. But this, too, will come with its own inherent risks and rewards."

Some companies are already monetizing their customers' personal data. Telecoms companies, for example, are using customer geolocation data (with permission) to tailor offerings from 3rd party vendors such as insurers and retailers; car 'communities' are being created around customer driving patterns. Yet continued expansion of these models will require that all those involved in the ecosystem are able to keep that data private, secure and confidential.

Those tech companies and IoT solutions developers that take a disciplined approach, investing the appropriate time and resources to integrate security, privacy and trust concepts into their IoT solutions will – ultimately – win out over those that eschew discipline in order to be first to market.

> "Security really needs to be designed into IoT solutions right at the start. You need to think about it at the hardware level, the firmware level, the software level and the service level. And you need to continuously monitor it and stay ahead of the threat."
>
> —Florence Hudson, Senior Vice President and Chief Innovation Officer Internet2 (formerly with IBM)

Looking for standards

Characterized by massive growth, wildfire adoption and rapidly emerging use cases, IoT is a virtual 'Wild West' with few rules, little regulatory oversight and masses of pioneers competing to strike their fortune. The industry, regulators and users will need to come together to form generally-accepted standards and ecosystems.

In part to improve the interoperability of IoT solutions and in part to help define the minimum expected security standards, many organizations now believe that the development of industry standards will be the single most important step to driving IoT adoption. Indeed, it is often not until generally-accepted standards are set that most new innovations truly achieve mainstream adoption.

Knowing this, many tech firms – both large and small – have started to create consortiums of like-minded organizations to help focus on creating and commercializing new standards. New consortiums and standards are being announced every few months, leading to tight competition and significant uncertainty for players in the market.

Google's Nest product, for example, has partnered with companies such as Samsung Electronics, ARM Holdings, Freescale Semiconductor and Silicon Labs to develop their 'Thread' networking protocol aimed at standardizing IoT communications in the home. At the same time, Intel has partnered with Cisco, AT&T, GE and IBM to create standards specifically for industrial IoT use. Cisco is also part of the AllSeen Alliance created by Qualcomm, alongside heavyweights such as Microsoft, LG and HTC to create an interoperable peer connectivity and communications framework. And in August 2015, the Online Trust Alliance was launched as a collaborative effort that includes firms such as Microsoft, Symantec, Target and ADT who plan to offer guidelines for IoT manufacturers, developers and retailers with a focus on consumer IoT devices.

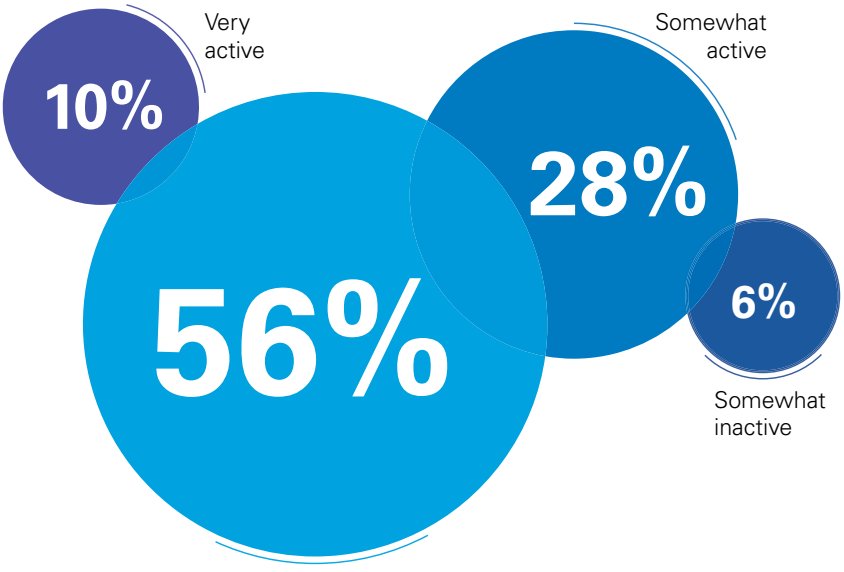
> “Companies need to stop thinking about regulation as a cost to manage and instead start taking a longer-term view. They need to be asking themselves how they can influence the development of regulation and how that impacts the emergence of the market and the success of the business.”
>
> —Dr. Michael Geist, Canada Research Chair, Internet and E-commerce Law, University of Ottawa

"This industry is very fragmented, with lots of standard and quasi-standard bodies addressing similar issues – thus aligning the industry around the same approach and standard requires a broad alignment and participation," noted Maciej Kranz, VP, Strategic Innovations, at Cisco.

Collaboration or competition?

Given the pervasiveness of IoT and the sensitivity of the systems and data, nobody active in the sector doubts the need for clear IoT regulation and standards. As Chris Wiegand, CEO of Jibestream notes, "It's the industry that

Most IoT user organizations are taking a laid back approach to driving the IoT debate



Source: 2015 KPMG Cyber Security and IoT Survey

Within your industry, how active a role has your firm taken in starting a dialogue about the IoT?

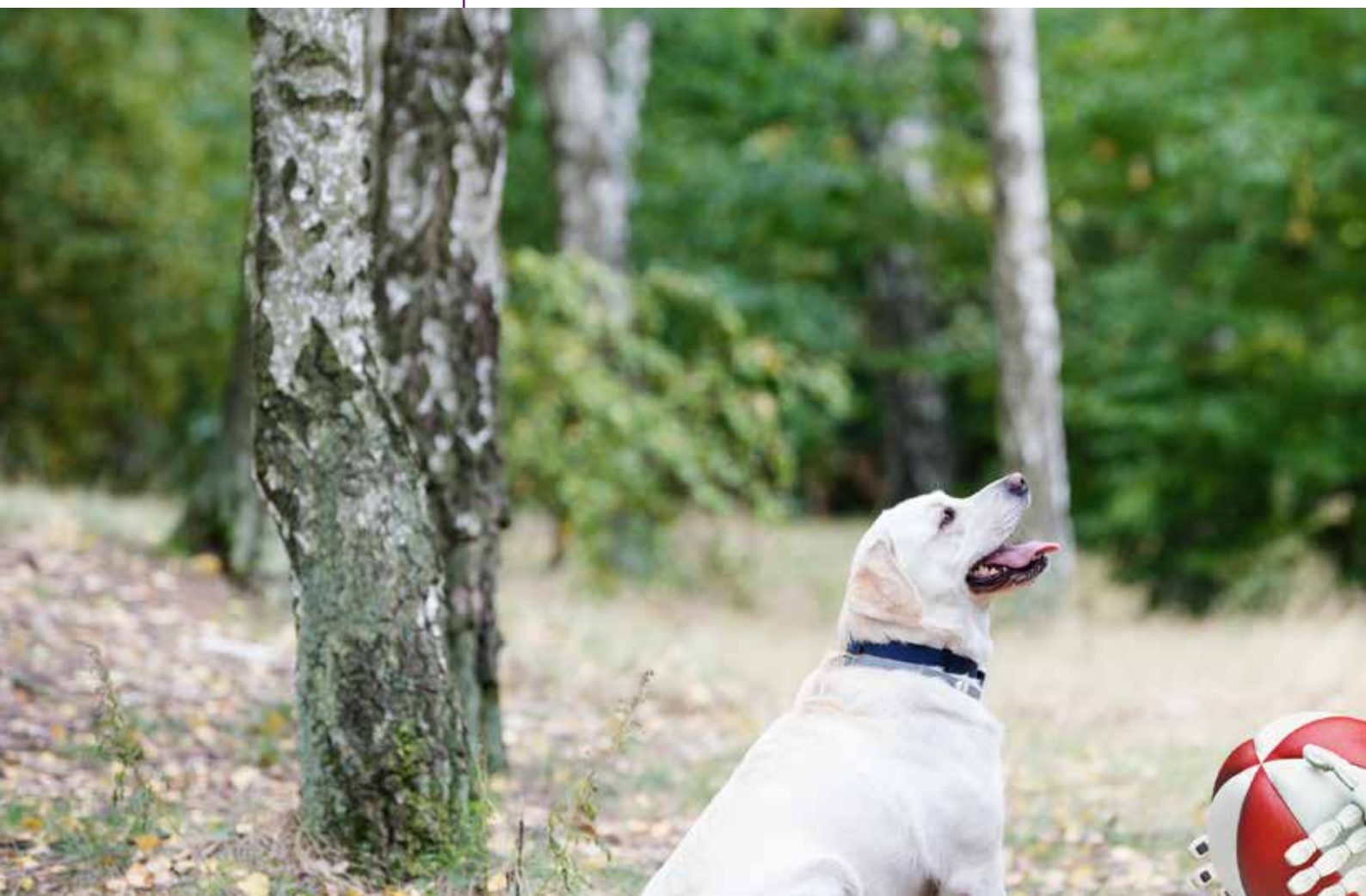
is really developing the Internet of Things and we need to ensure that we do it right and not in a way that exposes it to misuse or abuse."

However, there are some concerns among players that competition over standards will only harm the sector. As Internet2's Florence Hudson notes, "There is a splintering happening where everyone is trying to create consortiums, but everybody is also trying to win. So what I'm hoping is that we can create an eco-system across the industry at every point to develop these themes of security and privacy, and then use these consortiums as channels to execute it."

Increased regulatory oversight and guidance will also help drive forward adoption. Almost a third of companies already using an IoT solution said that the existing lack of rules and regulations were creating challenges to IoT adoption.

Those in highly regulated industries – financial services, healthcare and utilities, for example – have particular reason to be concerned.

"Regulators often have trouble catching up with new innovations and – until they do – often take a dim view of change within their sector; it is not surprising that many US healthcare organizations are looking to the FDA to tell them which wearable devices will be accepted within the US health sector," added Greg Bell, Principal and Services Leader, KPMG Cyber. "Regulation is a double edged sword – on the one side it requires organizations to invest in compliance and reporting but, at the same time, it also clarifies what will and won't be accepted, allowing organizations to move ahead with their investments and planning."



In some sectors, however, the lack of regulation may be slowing the adoption of IoT solutions. Many Tesla drivers, for example, now have access to an 'auto-pilot' feature which promises to reduce accidents and improve safety, which when matured to autonomous driving vehicles may even reduce accidents. But – to date – road regulators have been unwilling to allow the feature to be used on public roads, thereby severely limiting the competitive advantage gained through this novel technology.

More to do

Our experience suggests that few technology companies and IoT solutions developers are actively working towards creating standards. Fewer still are engaging with regulators to understand – and to inform – the direction of future regulatory travel.

"It seems that many of the smaller tech players in the ecosystem are simply standing on the sidelines waiting – along with their customers – to hear what standards and regulations will win the day; they are letting the bigger players make all the decisions," noted Malcolm Marshall, Global Leader, Cyber Security. "This is no time to take a passive stance. Tech firms should be out there working collaboratively with as many consortiums as they can to understand – and, where possible, influence – the various standards being created."

However, as Cisco's Maciej Kranz reiterates, "There's at least 10 to 15 different standard bodies that are thinking about each aspect of security, privacy and trust in IoT, and it's important that we consolidate these efforts and take a holistic approach versus each of the industries coming up with their best practices and standards."

Focus on security, privacy and trust

We believe that the most successful IoT solution providers and tech companies will likely be those that focus equally on improving security, protecting privacy and building trust. All three elements are key to building market-share in the IoT space.

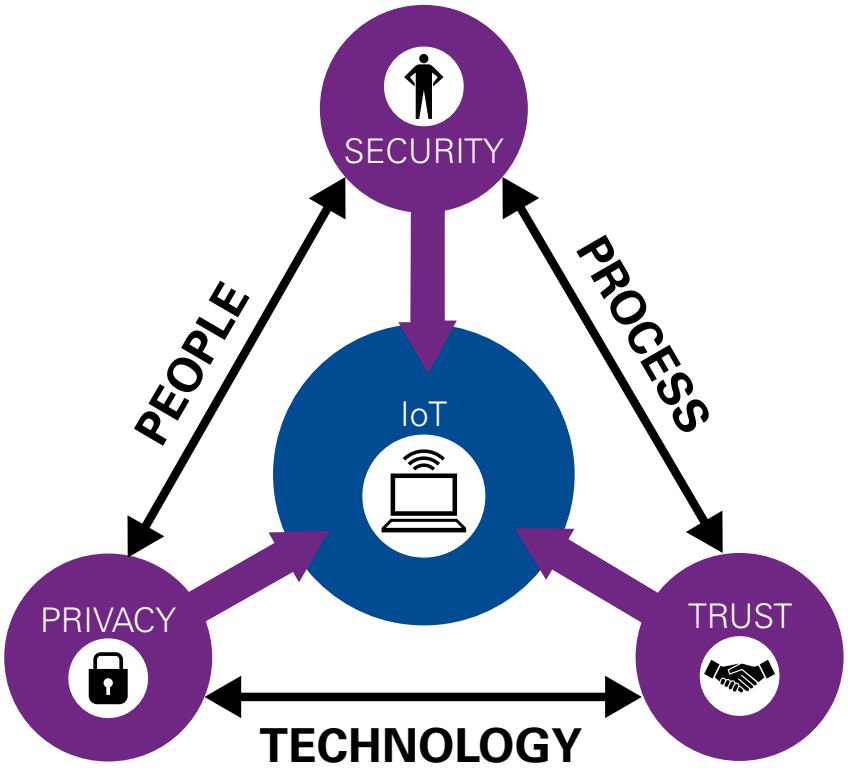
While the topic of cyber security certainly seems to be front and center for both IoT users and developers, our experience suggests that most are taking a rather narrow view of their obligations. We believe that a robust 'cyber security' approach focuses not only on protecting the devices and infrastructure that underpin the system, but also on developing the right level of data privacy and building trust with customers and regulators.

What is security, privacy and trust in the IoT ecosystem?

Often confused as a single concept, the reality is that successful IoT solutions, products and innovations will require tech firms and solutions developers to think more specifically about three key concepts that enable a valuable user experience: security, privacy and trust.

Security – often defined as an organization's ability to control their environment, devices and software – is most frequently discussed at industry conferences and meetings and can often be embedded into coding or manufacturing processes and updated regularly.

Privacy, on the other hand, relates to confidentiality and data control and – as such – can often be much more difficult to 'embed' into a solution or product.



Privacy isn't just about how you protect your customer data, it's also about how your customers allocate rights to their data and how that information is shared and used among 3rd parties.

The area that (to date) has been least frequently debated has been the impact of 'trust' on the IoT relationship. Much more than simply 'brand trust' and reputation, IoT developers and tech firms will need to build an 'ecosystem' of trust and integrity with their users, partners, suppliers and customers in order to create new and more value-driven opportunities for customers. In some cases, trust can be achieved by leveraging the virtues of an already-trusted 3rd party who protects the consumer or users.

We believe…

For security to be effective in IoT, it needs to be built into the technology and as close to the asset as possible: devices should have embedded security controls; software should have security embedded into the code. In fact, security should be a fail-safe control which means even when the technology is "off-line" it is still secure. What we don't recommend is building 'open' devices or creating platforms where security is controlled centrally. The risks are just too high.

> "They're going to try to hack everything," warns Florence Hudson of IBM. "I am most worried about security in healthcare, in cars and moving vehicles and in critical infrastructure."

Focus on security

Given the role that IoT devices are expected to play in the new world of tomorrow – managing everything from the temperature of the room to the speed of the car – it is surprising that the majority of IoT users have been slow to adopt many of the more traditional cyber security measures used in the market today.

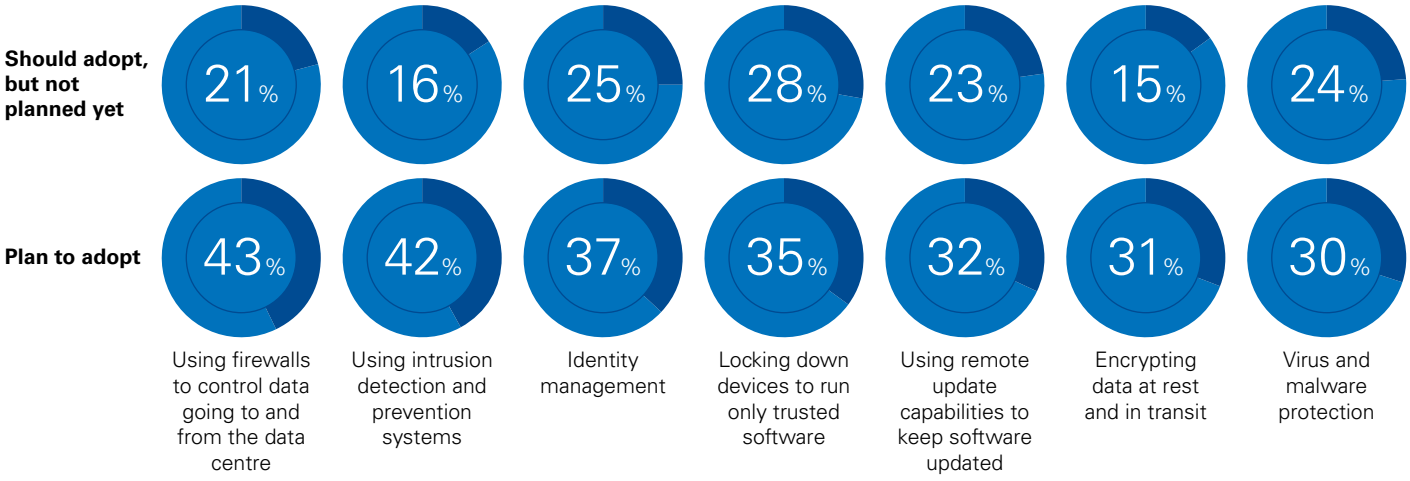
In our survey, only around 40 percent of companies currently using IoT said they had already implemented measures such as improving firewall controls, enhancing identify management processes and running intrusion software.

Yet attacks are already a reality. In 2014, ICS-Cert (a branch of the US Department of Homeland Security focused on cyber threats) reported a total of 245 incidents involving control systems (often the platform on which industrial IoT devices are integrated and controlled), of which 55 percent involved Advanced Persistent Threats (APT) – sophisticated attacks typically directed at high-value business targets; 42 percent of these targeted communication, water and transport infrastructure[2].

It seems clear that – as more and more devices shift online – threat actors will increase their efforts to overcome IoT security measures, whether for financial gain, political motivation, or simply to further exercise their skills and capabilities. And, as organizations start to rely more and more on IoT data, these targets will become increasingly attractive to these committed threat actors.

In order to deliver a safer and more secure IoT environment, tech companies and solutions developers will need to take a lead role in making their devices and solutions as secure as possible. "Security really needs to be carefully considered right at the design phase and then continuously tested and updated throughout the development process," noted Gary Matuszak, Global Chair, Technology, Media & Telecommunications. "Those that are able to add in 'after-market' updates and upgrades will not only deliver more value to their customers, they will also help maintain their own reputations in the market."

IoT users and solutions developers are hoping to leverage a broad basket of existing and potential technology solutions to respond to the risk of cyber-attack on their IoT solutions



Source: KPMG Cyber Security and IoT Survey

Of the following, which does your firm plan to adopt to tackle the security risks to IoT solutions?

2 https://ics-cert.us-cert.gov/monitors/ICS-MM201502

Focus on privacy

As today's consumers increasingly start to recognize the value that their personal information represents to companies and service providers, they are quickly becoming more comfortable with the idea of sharing personal information in return for improved service or lower prices.

However, underwriting this information-for-value covenant is a clear agreement on exactly what information can be shared, who it can be shared with and for what purpose. A consumer with a wearable and connected heart monitor, for example, would expect this information to be shared with their healthcare providers, but would likely not want it to be shared with marketers or health insurance plans.

Rather than just being a risk, however, the debate about privacy is quickly evolving to one of opportunity. Simply put, consumers are recognizing the value that their personal information offers – not only their transaction records, but also their behavioral data and their metadata – and are already essentially 'trading' their information to companies for better service, lower costs or promotions. This, in turn, is leading to new opportunities and potential value for IoT organizations.

"Personal information is quickly becoming a new form of currency for consumers and, in the right circumstances and for the right pay-off, IoT users will be happy to share their data," noted Henry Shek, Partner, KPMG in China. "But that means that IoT solutions providers, their corporate customers and everyone else in the IoT value chain will need to be very clear about what data can be shared and with whom."

We believe…

Organizations will start to negotiate with their users to gain permission to certain personal information in return for clear benefits. As such, tech companies and IoT developers have a unique opportunity to create and manage value-added services that both manages permissions and securely integrates and aggregates data.

We believe…

IoT will lead to greater integration between products and services – integrating traffic-aware mapping services into cars or developing payment applications for phones, for example – as organizations focus on providing a more complete and seamless quality experience to their end-users.

> "What's on most people's minds right now is keeping customer trust and issues surrounding privacy, security and integrity of data."
>
> —Danny Le, Partner, KPMG in the US

Focus on trust

Much like personal information can be converted into value for consumers, trust can be converted into value for tech firms and IoT solution providers. There is a mountain of literature that demonstrates the irrefutable connection between 'brand trust', customer experience and sales.

Products and services from brands that enjoy a high level of customer trust not only tend to have stronger 'relationships' with customers, they also enjoy broader latitude to cross-sell services and products. Consider, for example, how certain technology companies have been able to parlay their existing brand and customer trust in one service area into market dominance in an entirely new one – such as mobile payments – where, arguably, they had no prior experience or footprint at all. Clearly, customer trust is key to long-term success in the IoT space.

"In part, trust is based on your ability to maintain the security of the system and your ability to protect customer information, but it also must include considerations related to your brand image, the way you communicate with consumers and how you respond to unintended security or privacy breaches," added Richard Marriott, Senior Manager, Cyber Security KPMG in the UK. "You can't just assume that if you secure it, trust will come. You have to really work at building it."

We believe…

Some existing players will ultimately become the effective 'trust provider' within the ecosystems they operate in. The challenge will come when the 'trust provider' becomes the dominant brand rather than the device manufacturer or service provider thus, potentially, disintermediating the other players in the ecosystem.

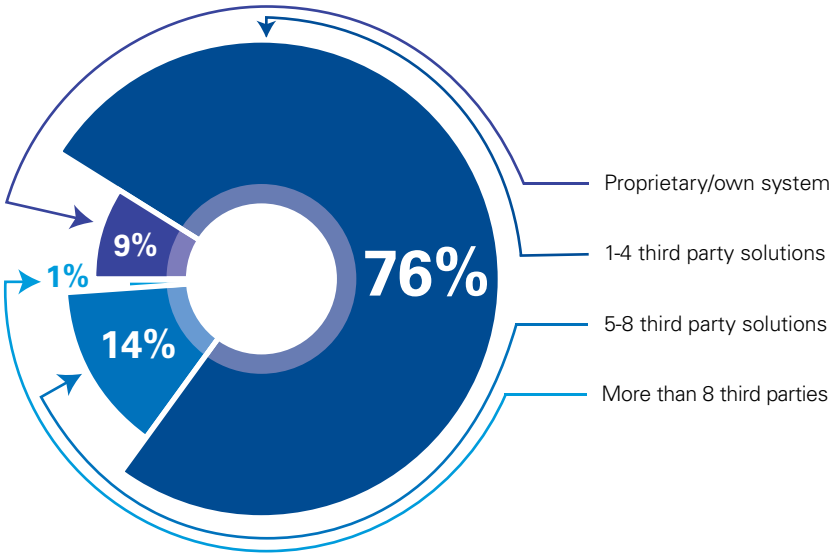
Driving security, privacy and trust across the ecosystem

No one company can 'go it alone' in the IoT space; success will require organizations to partner, value chains to be created and ecosystems to flourish. Yet as IoT users start to bring more players, service providers and 3rd party suppliers into their value chain, tech firms and IoT solutions providers will face increasing pressure to demonstrate their security capabilities.

From device manufacturers and infrastructure service providers through to telco companies and data warehousing facilities, it will take a wide variety of players to come together to create the right ecosystem for IoT. Already, more than three-quarters of current IoT users say they use between one and four 3rd parties to manage their IoT solutions; 15 percent say they use more than five 3rd parties.

"The reality is that none of the companies can do it alone. At Cisco, we're developing a large number of partnerships, both horizontal and vertical, to develop and deliver the platform capabilities and solutions," noted Cisco's Maciej Kranz.

The IoT ecosystem is growing and users increasingly understand that they need to rely on third parties and providers to develop a strong market proposition



Source: KPMG Cyber Security and IoT Survey

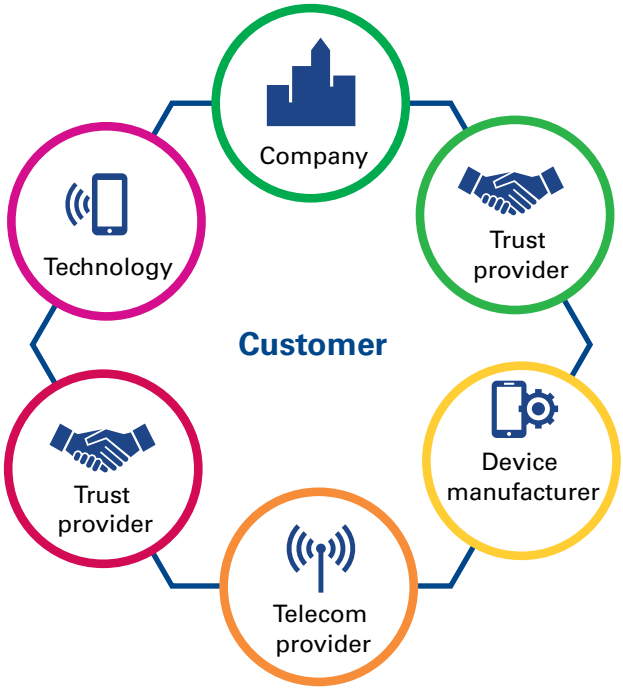
How many third parties are part of your IoT solution?

We believe…

The ecosystem will shift from a linear model with the customer at the end to one where the customer is in the middle and ecosystem participants orbit around them. In this environment, we expect to see traditional 'roles' start to shift as players start to take on different roles in the ecosystem and overall value proposition.

Then technology ecosystem used to be linear … .

In today's IoT ecosystem, players 'orbit' around the customer



However, our data suggests that few IoT users have fully considered how their new value chains will impact the overall security of their IoT solutions. In fact, 44 percent of our respondents admitted that they had not yet considered the way in which 3rd party partners perceive security risks.

"Cyber-attack on devices is a real risk right now and we have to mitigate that risk by choosing vendors that offer some level of management or security, and staying away from others that are kind of treating the whole IoT world as the Wild West right now," said Chris Wiegand of Jibestream.

Conversely, however, smaller start-ups and those with low brand recognition in the market may find that – by virtue of their partners in their ecosystem – they can build up their customer trust fairly quickly.

Assessing your 3rd parties

As the IoT market matures and adoption increases, however, we expect to see IoT users start to demand security, privacy, and trust assurances that all of the suppliers in the ecosystem also have policies and safeguards that align to those of the customer. In some cases, organizations are introducing technology and tools – such as remote process monitoring – to track supplier performance. Others are asking their suppliers to gain an accreditation or submit to audits to ensure alignment.

According to one North American CIO, "We have appointed an accredited evaluation party to assess the security standards of our external partners as an added responsibility and they have agreed to the same for a reasonable amount which fit our budget."

An increasingly common approach is to use 3rd party due diligence assessments and existing standards and attestation programs – such as the Service Organization Control Type 2 Assurance Reporting (SOC2), which tests and reports on the design and operational effectiveness of an organization's controls – to assess the security stance of 3rd parties. SOC 2 is based on five key 'trust service principles': security, availability, processing integrity, confidentiality and privacy. For example, in the US healthcare sector, SOC 2 is increasingly being used to ensure 3rd parties are not only maintaining a high level of security, privacy and trust, but also that they are compliant with key data security regulations such as HIPAA.

We believe…

All of the participants in the ecosystem must have a responsibility to protect the security, privacy and trust of the solution for the 'handshake' to work in order to protect the end-user.

5 key takeaways

1. **The IoT market is evolving.** The IoT sector is growing rapidly and will likely undergo several iterations of transformation. Similarly, concerns related to security, privacy and trust will also evolve and transform as the market changes. As such, security strategies should be broad-based to anticipate and respond to potential disruptions that could impact current market positions.

2. **The IoT eco-system plays a critical role in securing IoT.** Businesses should carefully evaluate their 3rd party suppliers, identify qualified partners, and invest in integrating security, privacy and trust across the ecosystem. Business should consider different approaches to building the capabilities they require within the ecosystem including whether they can buy, build, partner, invest, or create an alliance to achieve their goals.

3. **Security must be built-in from the ground up with the customer in mind.** Consumers and business partners will expect security to be built into the system; technology architects should follow an 'always-on' principle that provides high levels of control with appropriate fail-safes. Given the scale and velocity of IoT growth, security vulnerabilities can become large liabilities to the company.

4. **Look for opportunities to drive value from security.** Security architects should reconsider the security models to identify potential to enhance the value of security. Consider, for example, using premium concepts of security, privacy, and trust to differentiate the product. Security for IoT is not just about protecting valuable data, it's also about finding opportunities to monetize the intelligence.

5. **Engage in industry and regulatory groups to accelerate the normalization and standardization of IoT.** Collaboration will reduce ambiguity and accelerate a company's ability to launch products and services within a sustainable business ecosystem. At the same time, regulators will also need to participate in industry discussion in order to protect market and consumer interests. Technology companies should be proactive to help regulators to support IoT.

Contact us

For further information about this publication and on the services offered by KPMG's Technology, Media & Telecommunications practice, please contact:

Gary Matuszak
Global Chair
Technology, Media & Telecommunications
T: +1 408 367 4757
E: gmatuszak@kpmg.com

Greg Bell
Principal and Services Leader, KPMG Cyber
KPMG in the US
T: +1 404 222 7197
E: rgregbell@kpmg.com

Danny Le
Partner
KPMG in the US
T: +1 213 430 2139
E: dqle@kpmg.com

Acknowledgments

We would like to thank the following people for their valuable contribution to this study:

All survey respondents, Florence Hudson, Michael Geist, Bridget Karlin, Maciej Kranz, Chris Wiegand and our external writer Peter Schram.

KPMG's firms' partners and principals who provided their insight, including Malcolm Marshall, Richard Marriott, and Henry Shek.

The KPMG International project team: Sunitha Shivakumar, Alise Barnes, and Carolyn Forest.

kpmg.com

kpmg.com/socialmedia

kpmg.com/app

Designed by Evalueserve.

Publication name: Security and the IoT ecosystem

Publication number: 132631-G

Publication date: December 2015

- Author: Bruce Schneier. Bruce Schneier
- Date of Publication: 01.06.14. 01.06.14
- Time of Publication: 6:30 am. 6:30 am

The Internet of Things Is Wildly Insecure — And Often Unpatchable

We're at a crisis point now with regard to the security of embedded systems, where computing is embedded into the hardware itself — as with the Internet of Things. These embedded computers are riddled with vulnerabilities, and there's no good way to patch them.

It's not unlike what happened in the mid-1990s, when the insecurity of personal computers was reaching crisis levels. Software and operating systems were riddled with security vulnerabilities, and there was no good way to patch them. Companies were trying to keep vulnerabilities secret, and not releasing security updates quickly. And when updates were released, it was hard — if not impossible — to get users to install them. This has changed over the past twenty years, due to a combination of full disclosure — publishing vulnerabilities to force companies to issue patches quicker — and automatic updates: automating the process of installing updates on users' computers. The results aren't perfect, but they're much better than ever before.

But this time the problem is much worse, because the world is different: All of these devices are connected to the Internet. The computers in our routers and modems are much more powerful than the PCs of the mid-1990s, and the Internet of Things will put computers into all sorts of consumer devices. The industries producing these devices are even less capable of fixing the problem than the PC and software industries were.

If we don't solve this soon, we're in for a security disaster as hackers figure out that it's easier to hack routers than computers. At a recent Def Con, a researcher looked at thirty home routers and broke into half of them — including some of the most popular and common brands.

To understand the problem, you need to understand the embedded systems market.

Typically, these systems are powered by specialized computer chips made by companies such as Broadcom, Qualcomm, and Marvell. These chips are cheap, and the profit margins slim. Aside from price, the way the manufacturers differentiate themselves from each other is by features and bandwidth. They typically put a version of the Linux operating system onto the chips, as well as a bunch of other open-source and proprietary components and drivers. They do as little engineering as possible before shipping, and there's little incentive to update their "board support package" until absolutely necessary.

The system manufacturers — usually original device manufacturers (ODMs) who often don't get their brand name on the finished product — choose a chip based on price and features, and then build a router, server, or whatever. They don't do a lot of engineering, either. The brand-name company on the box may add a user interface and maybe some new features, make sure everything works, and they're done, too.

The problem with this process is that no one entity has any incentive, expertise, or even ability to patch the software once it's shipped. The chip manufacturer is busy shipping the next version of the chip, and the ODM is busy upgrading its product to work with this next chip. Maintaining the older chips and products just isn't a priority.

And the software is old, even when the device is new. For example, one survey of common home routers found that the software components were four to five years older than the device. The minimum age of the Linux operating system was four years. The minimum age of the Samba file system software: six years. They may have had all the security patches applied, but most likely not. No one has that job. Some of the components are so old that they're no longer being patched. This patching is especially important because security vulnerabilities are found "more easily" as systems age.

To make matters worse, it's often impossible to patch the software or upgrade the components to the latest version. Often, the complete source code isn't available. Yes, they'll have the source code to Linux and any other open-source components. But many of the device drivers and other components are just "binary blobs" — no source code at all. That's the most pernicious part of the problem: No one can possibly patch code that's just binary.

Even when a patch is possible, it's rarely applied. Users usually have to manually download and install relevant patches. But since users never get alerted about security updates, and don't have the expertise to manually administer these devices, it doesn't happen. Sometimes the ISPs have the ability to remotely patch routers and modems, but this is also rare.

The result is hundreds of millions of devices that have been sitting on the Internet, unpatched and insecure, for the last five to ten years.

Hackers are starting to notice. Malware DNS Changer attacks home routers as well as computers. In Brazil, 4.5 million DSL routers were compromised for purposes of financial fraud. Last month, Symantec reported on a Linux worm that targets routers, cameras, and other embedded devices.

This is only the beginning. All it will take is some easy-to-use hacker tools for the script kiddies to get into the game.

And the Internet of Things will only make this problem worse, as the Internet — as well as our homes and bodies — becomes flooded with new embedded devices that will be equally poorly maintained and unpatchable. But routers and modems pose a particular problem, because they're: (1) between users and the Internet, so turning them off is increasingly not an option; (2) more

powerful and more general in function than other embedded devices; (3) the one 24/7 computing device in the house, and are a natural place for lots of new features.

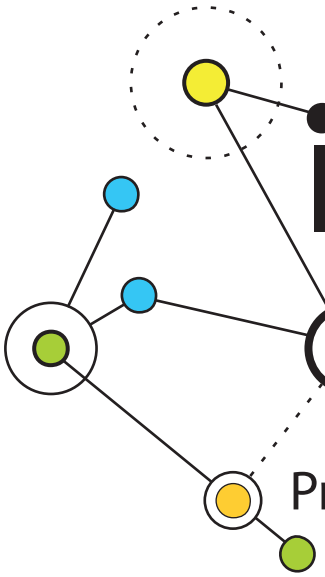
We were here before with personal computers, and we fixed the problem. But disclosing vulnerabilities in an effort to force vendors to fix the problem won't work the same way as with embedded systems. The last time, the problem was computers, ones mostly not connected to the Internet, and slow-spreading viruses. The scale is different today: more devices, more vulnerability, viruses spreading faster on the Internet, and less technical expertise on both the vendor and the user sides. Plus vulnerabilities that are impossible to patch.

Combine full function with lack of updates, add in a pernicious market dynamic that has inhibited updates and prevented anyone else from updating, and we have an incipient disaster in front of us. It's just a matter of when.

We simply have to fix this. We have to put pressure on embedded system vendors to design their systems better. We need open-source driver software — no more binary blobs! — so third-party vendors and ISPs can provide security tools and software updates for as long as the device is in use. We need automatic update mechanisms to ensure they get installed.

The economic incentives point to large ISPs as the driver for change. Whether they're to blame or not, the ISPs are the ones who get the service calls for crashes. They often have to send users new hardware because it's the only way to update a router or modem, and that can easily cost a year's worth of profit from that customer. This problem is only going to get worse, and more expensive. Paying the cost up front for better embedded systems is much cheaper than paying the costs of the resultant security disasters.

Editor: Sonal Chokshi @smc90

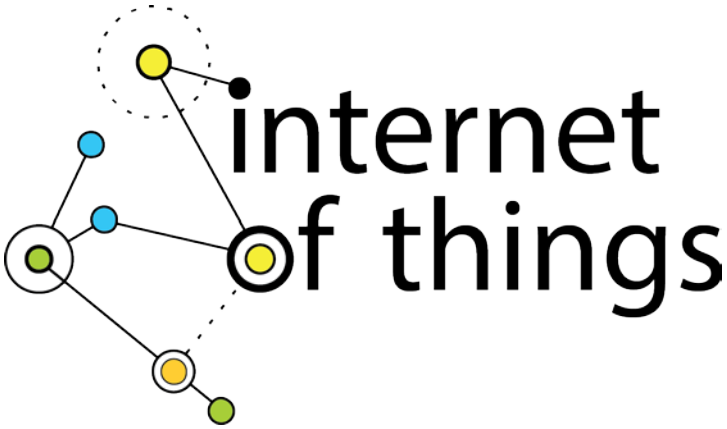


internet of things

Privacy & Security in a Connected World

FTC Staff Report

JANUARY 2015



FTC Staff Report
January 2015

Table of Contents

Executive Summary i

Background 1

What is the "Internet of Things"? 5

Benefits & Risks 7

- Benefits 7
- Risks 10

Application of Traditional Privacy Principles 19

- Summary of Workshop Discussions 19
- Post-Workshop Developments 25
- Commission Staff's Views and Recommendations for Best Practices 27

Legislation 47

- Summary of Workshop Discussions 47
- Recommendations 48

Conclusion 55

Executive Summary

The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day.

Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.

Given these developments, the FTC hosted a workshop on November 19, 2013 – titled *The Internet of Things: Privacy and Security in a Connected World*. This report summarizes the workshop and provides staff's recommendations in this area.[1] Consistent with the FTC's mission to protect consumers in the commercial sphere and the focus of the workshop, our discussion is limited to IoT devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, nor does it address broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Workshop participants discussed benefits and risks associated with the IoT. As to benefits, they provided numerous examples, many of which are already in use. In the health arena, connected medical devices can allow consumers with serious medical conditions to work

[1] Commissioner Wright dissents from the issuance of this Staff Report. His concerns are explained in his separate dissenting statement.

with their physicians to manage their diseases. In the home, smart meters can enable energy providers to analyze consumer energy use, identify issues with home appliances, and enable consumers to be more energy-conscious. On the road, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership. Participants generally agreed that the IoT will offer numerous other, and potentially revolutionary, benefits to consumers.

As to risks, participants noted that the IoT presents a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety. Participants also noted that privacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. In particular, some panelists noted that companies might use this data to make credit, insurance, and employment decisions. Others noted that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption.

In addition, workshop participants debated how the long-standing Fair Information Practice Principles ("FIPPs"), which include such principles as notice, choice, access, accuracy, data minimization, security, and accountability, should apply to the IoT space. The main discussions at the workshop focused on four FIPPs in particular: security, data minimization, notice, and choice. Participants also discussed how use-based approaches could help protect consumer privacy.

1. Security

There appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities. Commission staff encourages companies to consider adopting the best practices highlighted by workshop participants, including those described below.

First, companies should build security into their devices at the outset, rather than as an afterthought. As part of the security by design process, companies should consider: (1) conducting a privacy or security risk assessment; (2) minimizing the data they collect and retain; and (3) testing their security measures before launching their products. Second, with respect to personnel practices, companies should train all employees about good security, and ensure that security issues are addressed at the appropriate level of responsibility within the organization. Third, companies should retain service providers that are capable of maintaining reasonable security and provide reasonable oversight for these service providers. Fourth, when companies identify significant risks within their systems, they should implement a defense-in-depth approach, in which they consider implementing security measures at several levels. Fifth, companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network. Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.

2. Data Minimization

Data minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it. Although some participants expressed concern that requiring data minimization could curtail innovative uses of data, staff agrees with the participants who stated that companies should consider reasonably limiting their collection and retention of consumer data.

Data minimization can help guard against two privacy-related risks. First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from such an event. Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.

To minimize these risks, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. However, recognizing the need to balance future, beneficial uses of data with privacy protection, staff's recommendation on data minimization is a flexible one that gives companies many options. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data, as explained below.

3. Notice and Choice

The Commission staff believes that consumer choice continues to play an important role in the IoT. Some participants suggested that offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information without a user interface. However, staff believes that providing notice and choice remains important.

This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits. This principle applies equally to the Internet of Things.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface and recognizes that there is no one-size-fits-all approach. Some options include developing video tutorials, affixing QR codes on devices, and providing choices at point of sale, within set-up wizards, or in a privacy dashboard. Whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents. In addition, companies may want to consider using a combination of approaches.

Some participants expressed concern that even if companies provide consumers with choices only in those instances where the collection or use is inconsistent with context, such an

approach could restrict unexpected new uses of data with potential societal benefits. These participants urged that use limitations be considered as a supplement to, or in lieu of, notice and choice. With a use-based approach, legislators, regulators, self-regulatory bodies, or individual companies would set "permissible" and "impermissible" uses of certain consumer data.

Recognizing concerns that a notice and choice approach could restrict beneficial new uses of data, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. In addition, if a company collects a consumer's data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. Furthermore, the Commission protects privacy through a use-based approach, in some instances. For example, it enforces the Fair Credit Reporting Act, which restricts the permissible uses of consumer credit report information under certain circumstances. The Commission also applies its unfairness authority to challenge certain harmful uses of consumer data.

Staff has concerns, however, about adopting a pure use-based model for the Internet of Things. First, because use-based limitations are not comprehensively articulated in legislation, rules, or widely-adopted codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful. Second, use limitations alone do not address the privacy and security

risks created by expansive data collection and retention. Finally, a pure use-based model would not take into account consumer concerns about the collection of sensitive information.[2]

The establishment of legislative or widely-accepted multistakeholder frameworks could potentially address some of these concerns. For example, a framework could set forth permitted or prohibited uses. In the absence of consensus on such frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

4. Legislation

Participants also discussed whether legislation over the IoT is appropriate, with some participants supporting legislation, and others opposing it. Commission staff agrees with those commenters who stated that there is great potential for innovation in this area, and that IoT-specific legislation at this stage would be premature. Staff also agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, in light of the ongoing threats to data security and the risk that emerging IoT technologies might amplify these threats, staff reiterates the Commission's previous recommendation for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach. General data security legislation should protect against unauthorized access to both personal information and device functionality itself. For

[2] In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards, which the Commission previously recommended in its 2012 privacy report. Although the Commission currently has authority to take action against some IoT-related practices, it cannot mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness. Commission staff thus again recommends that Congress enact broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as how to provide choices to consumers about data collection and use practices.[3]

In the meantime, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
  The Commission enforces the FTC Act, the FCRA, the health breach notification provisions of the HI-TECH Act, the Children's Online Privacy Protection Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws.

- **Consumer and business education:**
  The Commission staff will develop new consumer and business education materials in this area.

[3] Commissioner Ohlhausen does not agree with the recommendation for baseline privacy legislation. *See infra* note 191.

- **Participation in multi-stakeholder groups:**
  Currently, Commission staff is participating in multi-stakeholder groups that are considering guidelines related to the Internet of Things, including on facial recognition and smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers.

- **Advocacy:**
  Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area.

Background

Technology is quickly changing the way we interact with the world around us. Today, companies are developing products for the consumer market that would have been unimaginable a decade ago: Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. These are all examples of the Internet of Things ("IoT"), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people. The IoT explosion is already around us, in the form of wearable computers, smart health trackers, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn't a mobile phone, tablet, or traditional computer.

Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people.[1] Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.[2] Some estimate that by 2020, 90% of consumer cars will have an Internet connection, up from less than 10 percent in 2013.[3] Three and one-half billion sensors already are in the

[1] DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. These estimates include all types of connected devices, not just those aimed at the consumer market.

[2] *Id*.

[3] TELEFONICA, CONNECTED CAR INDUSTRY REPORT 2013 9 (2013), *available at* http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.

marketplace,[4] and some experts expect that number to increase to trillions within the next decade.[5] All of these connected machines mean much more data will be generated: globally, by 2018, mobile data traffic will exceed fifteen exabytes – about 15 quintillion bytes – each month.[6] By comparison, according to one estimate, an exabyte of storage could contain 50,000 years' worth of DVD-quality video.[7]

These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases. Home automation systems will enable consumers to turn off the burglar alarm, play music, and warm up dinner right before they get home from work. Connected cars will notify first responders in the event of an accident. And the Internet of Things may bring benefits that we cannot predict.

However, these connected devices also will collect, transmit, store, and potentially share vast amounts of consumer data, some of it highly personal. Given the rise in the number and types of connected devices already or soon to be on the market, the Federal Trade Commission ("FTC" or "Commission") announced in April 2013 that it would host a workshop on the privacy and security issues associated with such devices and requested public input about the issues to

---

[4] *See* Stanford Univ., *TSensors Summit™ for Trillion Sensor Roadmap* 1 (Oct. 23-25, 2013), *available at* http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf.

[5] *Id*.

[6] CISCO, CISCO VISUAL NETWORKING INDEX: GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2013–2018 3 (2014), *available at* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

[7] University of Bristol, Exabyte Informatics, *available at* http://www.bris.ac.uk/research/themes/exabyte-informatics.html.

consider.[8] In response to the request for comment, staff received twenty-nine public comments[9] from a variety of consumer advocacy groups, academics, and industry representatives. The workshop – titled *The Internet of Things: Privacy and Security in a Connected World* – took place on November 19, 2013, and featured panels of academics, researchers, consumer advocates, and representatives from government and industry.[10]

The workshop consisted of four panels,[11] each of which focused on a different aspect of the IoT.[12] The first panel, "The Smart Home,"[13] looked at an array of connected devices, such as home automation systems and smart appliances. The second panel, "Connected Health and Fitness,"[14] examined the growth of increasingly connected medical devices and health and fitness products, ranging from casual wearable fitness devices to connected insulin pumps. The third panel, "Connected Cars,"[15] discussed the different technologies involved with connected

---

[8] Press Release, FTC, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/04/ftc-seeks-input-privacy-and-security-implications-internet-things.

[9] Pre-workshop comments ("#484 cmt.") are available at http://www.ftc.gov/policy/public-comments/initiative-484.

[10] For a description of the workshop, *see* http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[11] In addition to the four panels, workshop speakers included Keith Marzullo of the National Science Foundation ("Marzullo"), who gave an overview of the IoT space (Transcript of Workshop at 15-34); Carolyn Nguyen ("Nguyen") of Microsoft Corp., who discussed contextual privacy and its implications for the IoT (Transcript of Workshop at 35-51); and Vinton "Vint" Cerf ("Cerf") of Google Inc., who gave the workshop's Keynote Address (Transcript of Workshop at 118-153).

[12] A complete transcript of the proceeding is available at http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf. Videos of the workshop also are available at http://www.ftc.gov/news-events/audio-video/ftc-events.

[13] Transcript of Workshop at 52-115.

[14] *Id.* at 164-234.

[15] *Id.* at 235-291.

cars, including Event Data Recorders ("EDRs")[16] and other vehicle "telematics," a term that refers to data collection, transmission, and processing technologies for use in vehicles. Finally, the fourth panel, "Privacy and Security in a Connected World,"[17] discussed the broader privacy and security issues raised by the IoT.

Following the workshop, the Commission invited comments on the issues raised by the panels.[18] In response, staff received seventeen public comments from private citizens, trade organizations, and privacy advocates.[19]

This report summarizes the workshop and provides staff's recommendations in this area. Section II of this report discusses how we define the "Internet of Things." Section III describes some of the benefits and risks of the new technologies that are part of the IoT phenomenon. Section IV examines the application of existing privacy principles to these new technologies, and Section V addresses whether legislation would be appropriate in this area. Sections IV and V begin by discussing the views of written commenters and workshop speakers (collectively, "participants"), and then set forth staff recommendations. These recommendations focus on the types of products and services consumers are likely to encounter today and in the foreseeable future. We look forward to continuing to explore privacy issues as new IoT technologies come to market.

---

[16] An EDR is "a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (*e.g.*, vehicle speed vs. time) or during a crash event . . . intended for retrieval after the crash event." 49 C.F.R. § 563.5.

[17] Transcript of Workshop at 292-364.

[18] Press Release, FTC, FTC Seeks Comment on Issues Raised at Internet of Things Workshop (Dec. 11, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-seeks-comment-issues-raised-internet-things-workshop.

[19] Post-workshop comments ("#510 cmt.") are available at http://www.ftc.gov/policy/public-comments/initiative-510.

What is the "Internet of Things"?

Although the term "Internet of Things" first appeared in the literature in 2005,[20] there is still no widely accepted definition.[21] One participant described the IoT as the connection of "physical objects to the Internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing."[22] Another participant described it as including "embedded intelligence" in individual items that can detect changes in their physical state.[23] Yet another participant, noting the lack of an agreed-upon definition of the IoT, observed, "[w]hat all definitions of IoT have in common is that they focus on how computers, sensors, and objects interact with one another and process data."[24]

The IoT includes consumer-facing devices, as well as products and services that are not consumer-facing, such as devices designed for businesses to enable automated communications between machines. For example, the term IoT can include the type of Radio Frequency Identification ("RFID") tags that businesses place on products in stores to monitor inventory; sensor networks to monitor electricity use in hotels; and Internet-connected jet engines and drills on oil rigs. Moreover, the "things" in the IoT generally do not include desktop or laptop computers and their close analogs, such as smartphones and tablets, although these devices are often employed to control or communicate with other "things."

---

[20] *See* Remarks of Marzullo, Transcript of Workshop at 19.

[21] *See Comment of ARM/AMD*, #510 cmt. #00018 at 1.

[22] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 1.

[23] Remarks of Marzullo, Transcript of Workshop at 19.

[24] *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 3.

For purposes of this report, we use the term IoT to refer to "things" such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet. Consistent with the FTC's mission to protect consumers in the commercial sphere, our discussion of IoT is limited to such devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, such as sensors in hotel or airport networks; nor does it discuss broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Benefits & Risks

Like all technologies, the Internet of Things has benefits and risks. To develop policy approaches to this industry, one must understand both. Below is a summary of the benefits and risks of IoT, both current and potential, highlighted by workshop participants.

Benefits

Most participants agreed that the IoT will offer numerous, and potentially revolutionary, benefits to consumers.[25] One area in which these benefits appear highly promising is health care.[26] For example, insulin pumps and blood-pressure cuffs that connect to a mobile app can enable people to record, track, and monitor their own vital signs, without having to go to a doctor's office. This is especially beneficial for aging patients, for whom connected health devices can provide "treatment options that would allow them to manage their health care at home without the need for long-term hospital stays or transition to a long-term care facility."[27] Patients can also give caregivers, relatives, and doctors access to their health data through these apps, resulting in numerous benefits. As one panelist noted, connected health devices can "improve quality of life and safety by providing a richer source of data to the patient's doctor for diagnosis and treatment[,] . . . improve disease prevention, making the healthcare system more efficient and driving costs down[,] . . . [and] provide an incredible wealth of data, revolutionizing

[25] *See Comment of Future of Privacy Forum*, #484 cmt. #00013 at 4; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 2.

[26] *See Comment of AT&T Inc.*, #484 cmt. #00004 at 5.

[27] *Comment of Med. Device Privacy Consortium*, #484 cmt. #00022 at 1.

medical research and allowing the medical community to better treat, and ultimately eradicate, diseases."[28]

Recent studies demonstrate meaningful benefits from connected medical devices. One workshop participant said that "one of the most significant benefits that we have from this connected world [is] the ability to . . . draw the patients in and engage them in their own care."[29] Another participant described a clinical trial showing that, when diabetic patients used connected glucose monitors, and their physicians received that data, those physicians were five times more likely to adjust medications, resulting in better disease management and substantial financial savings for patients. He stated that the clinical trial demonstrated that diabetic patients using the connected glucose monitor reduced their average blood sugar levels by two points and that, by comparison, the Food and Drug Administration ("FDA") considers medications that reduce blood sugar by as little as one half point to be successful.[30]

Consumers can benefit from the IoT in many other ways. In the home, for example, smart meters can enable energy providers to analyze consumer energy use and identify issues with home appliances, "even alerting homeowners if their insulation seems inadequate compared to that of their neighbors,"[31] thus empowering consumers to "make better decisions about how they use electricity."[32] Home automation systems can provide consumers with a "single platform that

[28] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 16.

[29] *See* Remarks of Stan Crosley, Indiana Univ. ("Crosley"), Transcript of Workshop at 199.

[30] *See* Remarks of Anand Iyer, WellDoc Communications, Inc. ("Iyer"), Transcript of Workshop at 188–189.

[31] *Comment of AT&T Inc.*, #484 cmt. #00004 at 4-5.

[32] Remarks of Eric Lightner, Department of Energy ("Lightner"), Transcript of Workshop at 54.

can connect all of the devices within the home, [with] a single app for controlling them."[33] Connected ovens allow consumers to "set [their] temperatures remotely . . . , go from bake to broil . . . , [and] monitor [their] products from various locations inside . . . and outside [their] home[s]."[34] Sensors known as "water bugs" can notify consumers if their basements have flooded,[35] and wine connoisseurs can monitor the temperature in their wine cellars to preserve their finest vintages.[36]

On the road, connected cars will increasingly offer many safety and convenience benefits to consumers. For example, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership.[37] Connected cars also can "offer real-time vehicle diagnostics to drivers and service facilities; Internet radio; navigation, weather, and traffic information; automatic alerts to first responders when airbags are deployed; and smartphone control of the starter and other aspects of the car."[38] In the future, cars will even drive themselves. Participants discussed the ability of self-driving cars to create safety benefits. For example, rather than having error-prone humans decide which car should go first at a four-way stop sign, self-driving cars will be able to figure out who should

[33] Remarks of Jeff Hagins, SmartThings ("Hagins"), Transcript of Workshop at 64.

[34] Remarks of Michael Beyerle, GE Appliances ("Beyerle"), Transcript of Workshop at 60.

[35] *See* Remarks of Scott Peppet, Univ. of Colorado School of Law ("Peppet"), Transcript of Workshop at 167.

[36] *See* Remarks of Cerf, Transcript of Workshop at 132.

[37] *See* Remarks of Christopher Wolf, Future of Privacy Forum ("Wolf"), Transcript of Workshop at 247-48.

[38] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 13.

go first according to a standard protocol.[39] They would also allow people with visual impairments to use their own cars as a mode of transportation.[40]

Risks

Despite these important benefits, there was broad agreement among participants that increased connectivity between devices and the Internet may create a number of security and privacy risks.[41]

SECURITY RISKS

According to panelists, IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT, as explained further below.

First, on IoT devices, as with desktop or laptop computers, a lack of security could enable intruders to access and misuse personal information collected and transmitted to or from the

---

[39] *See* Remarks of Cerf, Transcript of Workshop at 127.

[40] *See id.* at 138.

[41] *See, e.g.*, Remarks of Craig Heffner, Tactical Network Solutions ("Heffner"), Transcript of Workshop at 73-77, 109-10; Remarks of Lee Tien, Electronic Frontier Foundation ("Tien"), Transcript of Workshop at 82-83; Remarks of Hagins, Transcript of Workshop at 92-93, 110; Remarks of Jay Radcliffe, InGuardians, Inc. ("Radcliffe"), Transcript of Workshop at 182-84; Remarks of Iyer, Transcript of Workshop at 223; Remarks of Tadayoshi Kohno, Univ. of Washington ("Kohno"), Transcript of Workshop at 244-47, 263-64; Remarks of David Jacobs, Electronic Privacy Information Center ("Jacobs"), Transcript of Workshop at 296; Remarks of Marc Rogers, Lookout, Inc. ("Rogers"), Transcript of Workshop at 344-45. *See also, e.g.*, HP, INTERNET OF THINGS RESEARCH STUDY 5 (2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en ("HP Security Research reviewed 10 of the most popular devices in some of the most common IoT niches revealing an alarmingly high average number of vulnerabilities per device. Vulnerabilities ranged from Heartbleed to denial of service to weak passwords to cross-site scripting."); *id.* at 4 (noting that 80 percent of devices tested raised privacy concerns).

device. For example, new smart televisions enable consumers to surf the Internet, make purchases, and share photos, similar to a laptop or desktop computer. [42] Like a computer, any security vulnerabilities in these televisions could put the information stored on or transmitted through the television at risk. If smart televisions or other devices store sensitive financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud.[43] Thus, as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.[44]

Second, security vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems.[45] For example,

---

[42] *See, e.g.*, Erica Fink & Laurie Segall, *Your TV might be watching you*, CNN MONEY (Aug. 1, 2013), *available at* http://money.cnn.com/2013/08/01/technology/security/tv-hack/index.html ("Today's high-end televisions are almost all equipped with 'smart' PC-like features, including Internet connectivity, apps, microphones and cameras.").

[43] *See* Mario Ballano Barcena *et al.*, *Security Response, How safe is your quantified self?*, SYMANTEC (Version 1.1 – Aug. 11, 2014), *available at* www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf (noting risks relating to IoT including identity theft). According to the most recent statistics from the Bureau of Justice Statistics of the Department of Justice, an estimated 16.6 million Americans – about seven percent of Americans sixteen or older – experienced at least one incident of identity theft in 2012. Losses due to personal identity theft totaled $24.7 billion, billions of dollars more than the losses for all other property crimes *combined*. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2012 (Dec. 2013)), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf. Another study demonstrated that one in four people who received notice of a breach involving their personal information were victims of identity theft, a significantly higher figure than for individuals who did not receive a breach notice. *See* Javelin, 2013 Identity Fraud Report, *available at* https://www.javelinstrategy.com/brochure/276.

[44] *See, e.g.*, Remarks of Marzullo, Transcript of Workshop at 18-19 (discussing ubiquitous or pervasive computing); *id.* at 28-30 (discussing potential security vulnerabilities in devices ranging from pacemakers to automobiles); Remarks of Nguyen, Transcript of Workshop at 35 ("the first thing that really comes to mind are the sensors that are expected to be ubiquitously present and the potential for everything inanimate, whether it be in the home, in the car, or attached to the individual, to measure and transmit data").

[45] *See* Remarks of Heffner, Transcript at 113 ("[I]f I, as someone out on the Internet, can break into a device that is inside your network, I am now inside your network and I can access other things that you do care about . . . . There should never be a device on your network that you shouldn't care about the security of.").

a compromised IoT device could be used to launch a denial of service attack.[46] Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks.[47] Another possibility is that a connected device could be used to send malicious emails.[48]

Third, unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases. One participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine.[49] Another participant discussed a set of experiments where an attacker could gain "access to the car's internal computer network without ever physically touching the car."[50] He described how he was able to hack into a car's built-in telematics unit and control the vehicle's engine and braking, although he noted that "the risk to car owners today is incredibly small," in part because "all the automotive manufacturers that I know of are proactively trying to address these things."[51] Although the risks currently may be small, they could be amplified as fully

---

[46] *See, e.g.*, Dick O'Brien, *The Internet of Things: New Threats Emerge in a Connected World*, SYMANTEC (Jan. 21, 2014), *available at* www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world (describing worm attacking IoT devices that connects them to a botnet for use in denial of service attacks).

[47] *Id.*

[48] *See* Paul Thomas, *Despite the News, Your Refrigerator is Not Yet Sending Spam*, SYMANTEC (Jan. 23, 2014), *available at* http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam (debunking reports that an Internet worm had used compromised IoT devices to send out spam, but adding, "While malware for IoT devices is still in its infancy, IoT devices are susceptible to a wide range of security concerns. So don't be surprised if, in the near future, your refrigerator actually does start sending spam.").

[49] *See* Remarks of Radcliffe, Transcript of Workshop at 182. *See also* Remarks of Tien, Transcript of Workshop at 82-83 ("And obviously one of the big differences between, say, a problem with your phone and a problem with your . . . diabetes pump or your defibrillator is that if it is insecure and it is subject to any kind of malware or attack, it is much more likely there would be very serious physical damage.").

[50] Remarks of Kohno, Transcript of Workshop at 245.

[51] *See id.* at 245-47, 266.

automated cars, and other automated physical objects, become more prevalent. Unauthorized access to Internet-connected cameras or baby monitors also raises potential physical safety concerns.[52] Likewise, unauthorized access to data collected by fitness and other devices that track consumers' location over time could endanger consumers' physical safety. Another possibility is that a thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home.

These potential risks are exacerbated by the fact that securing connected IoT devices may be more challenging than securing a home computer, for two main reasons. First, as some panelists noted, companies entering the IoT market may not have experience in dealing with security issues.[53] Second, although some IoT devices are highly sophisticated, many others may be inexpensive and essentially disposable.[54] In those cases, if a vulnerability were discovered after manufacture, it may be difficult or impossible to update the software or apply a patch.[55] And if an update is available, many consumers may never hear about it.[56] Relatedly, many

---

[52] *See* discussion of TRENDnet, *infra* notes 132-34 and accompanying text (FTC settlement alleging that hackers were able to access video streams from TRENDnet cameras). In another notorious incident, a hacker gained access to a video and audio baby monitor. *See* Chris Matyszczyk, *Hacker Shouts at Baby Through Baby Monitor*, CNET (Apr. 29, 2014), *available at* www.cnet.com/news/hacker-shouts-at-baby-through-baby-monitor/. *See also* Kashmir Hill, *'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users*, FORBES (Aug. 27, 2013), *available at* www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/ (recounting a similar incident).

[53] Remarks of Tien, Transcript of Workshop at 71; Remarks of Heffner, Transcript of Workshop at 73-75; Remarks of Hagins, Transcript of Workshop at 92-93.

[54] *See Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2.

[55] *See, e.g.*, Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 9 (Sept. 16, 2014) ("Article 29 Working Group Opinion"), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf ("For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries.").

[56] *Id. See also* Hill, *supra* note 52 (noting that some 40,000 of 46,000 purchasers of connected cameras had not installed a firmware update addressing a security vulnerability).

companies – particularly those developing low-end devices – may lack economic incentives to provide ongoing support or software security updates at all, leaving consumers with unsupported or vulnerable devices shortly after purchase.[57]

PRIVACY RISKS

In addition to risks to security, participants identified privacy risks flowing from the Internet of Things. Some of these risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information – risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time,[58] which may allow an entity that has not directly collected sensitive information to infer it.

The sheer volume of data that even a small number of devices can generate is stunning: one participant indicated that fewer than 10,000 households using the company's IoT home-automation product can "generate 150 million discrete data points a day"[59] or approximately one data point every six seconds for each household.[60]

---

[57] *See, e.g.*, *Bruce Schneier, The Internet of Things Is Wildly Insecure — And Often Unpatchable*, WIRED (Jan. 6, 2014), *available at* http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem ("The problem with this process is that no one entity has any incentive, expertise, or even ability to patch the software once it's shipped. The chip manufacturer is busy shipping the next version of the chip, and the [original device manufacturer] is busy upgrading its product to work with this next chip. Maintaining the older chips and products just isn't a priority.").

[58] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 67; *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 4-5.

[59] Remarks of Hagins, Transcript of Workshop at 89.

[60] *Cf. infra* note 73 and accompanying text (discussing inferences possible from smart meter readings taken every two seconds).

Such a massive volume of granular data allows those with access to the data to perform analyses that would not be possible with less rich data sets.[61] According to a participant, "researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics (*e.g.*, gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement."[62] This participant noted that such inferences could be used to provide beneficial services to consumers, but also could be misused. Relatedly, another participant referred to the IoT as enabling the collection of "sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals."[63] Some panelists cited to general privacy risks associated with these granular information-collection practices, including the concern that the trend towards abundant collection of data creates a "non-targeted dragnet collection from devices in the environment."[64]

Others noted that companies might use this data to make credit, insurance, and employment decisions.[65] For example, customers of some insurance companies currently may opt into programs that enable the insurer to collect data on aspects of their driving habits – such

---

[61] *See* Article 29 Working Group Opinion, *supra* note 55, at 8 ("Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.").

[62] Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 115-16 (2014) (citations omitted) ("*Regulating the Internet of Things*"), *available at* http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf. Although we do not include smartphones in our definition of IoT (*see supra* p. 6), many IoT devices contain sensors similar to the sensors in smartphones, and therefore, similar types of inferences may be possible using data from IoT devices.

[63] *Comment of Elec. Privacy Info. Ctr.*, #484 cmt. #00011 at 3.

[64] Remarks of Tien, Transcript of Workshop at 67.

[65] *See* Remarks of Peppet, Transcript of Workshop at 169.

as in one case, the number of "hard brakes," the number of miles driven, and the amount of time spent driving between midnight and 4 a.m. – to help set the insurance rate.[66] Use of data for credit, insurance, and employment decisions could bring benefits – *e.g.*, enabling safer drivers to reduce their rates for car insurance or expanding consumers' access to credit – but such uses could be problematic if they occurred without consumers' knowledge or consent, or without ensuring accuracy of the data.

As a further example, one researcher has hypothesized that although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user's suitability for credit or employment (*e.g.*, a conscientious exerciser is a good credit risk or will make a good employee).[67] According to one commenter, it would be of particular concern if this type of decision-making were to systematically bias companies against certain groups that do not or cannot engage in the favorable conduct as much as others or lead to discriminatory practices against protected classes.[68]

Participants noted that the Fair Credit Reporting Act ("FCRA")[69] imposes certain limits on the use of consumer data to make determinations about credit, insurance, or employment, or for similar purposes.[70] The FCRA imposes an array of obligations on entities that qualify as

---

[66] *See* Peppet, *Regulating the Internet of Things*, *supra* note 62, at 106-07. *See also*, *e.g.*, Progressive, Snapshot Common Questions, *available at* http://www.progressive.com/auto/snapshot-common-questions/; StateFarm, Drive Safe & Save with In-Drive, *available at* https://www.statefarm.com/insurance/auto/discounts/drive-safe-save/indrive.

[67] *See* Remarks of Peppet, Transcript of Workshop at 167-169.

[68] *See id.* at 93, 123-24.

[69] 15 U.S.C. § 1681 *et seq*.

[70] *See*, *e.g.*, Remarks of Crosley, Transcript of Workshop at 213; Remarks of Peppet, Transcript of Workshop at 213; Peppet, *Regulating the Internet of Things*, *supra* note 62, at 126-127.

consumer reporting agencies, such as employing reasonable procedures to ensure maximum possible accuracy of data and giving consumers access to their information.[71] However, the FCRA excludes most "first parties" that collect consumer information; thus, it would not generally cover IoT device manufacturers that do their own in-house analytics. Nor would the FCRA cover companies that collect data directly from consumers' connected devices and use the data to make in-house credit, insurance, or other eligibility decisions – something that could become increasingly common as the IoT develops. For example, an insurance company may offer consumers the option to submit data from a wearable fitness tracker, in exchange for the prospect of lowering their health insurance premium. The FCRA's provisions, such as those requiring the ability to access the information and correct errors, may not apply in such circumstances.

Yet another privacy risk is that a manufacturer or an intruder could "eavesdrop" remotely, intruding into an otherwise private space. Companies are already examining how IoT data can provide a window into the previously private home.[72] Indeed, by intercepting and analyzing unencrypted data transmitted from a smart meter device, researchers in Germany were

---

[71] *See* 15 U.S.C. §§1681e, 1681j.

[72] *See, e.g.*, Louise Downing, *WPP Unit, Onzo Study Harvesting Smart-Meter Data*, BLOOMBERG (May 12, 2014), *available at* http://origin-www.bloomberg.com/apps/news?pid=conewsstory&tkr=WPP:LN&sid=aPY7EUU9oD6g (reporting that the "world's biggest advertising agency" and a software company are collaborating to explore uses of smart meter data and quoting a CEO who noted, "Consumers are leaving a digital footprint that opens the door to their online habits and to their shopping habits and their location, and the last thing that is understood is the home, because at the moment, when you shut the door, that is it."). *See also Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2-3 ("to the extent that a powerful commercial entity controls an IoT networking platform within a home or business, that positions them to collect, analyze, and act upon copious amounts of data from within traditionally private spaces.").

able to determine what television show an individual was watching.[73] Security vulnerabilities in camera-equipped devices have also raised the specter of spying in the home.[74]

Finally, some participants pointed out that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential and may result in less widespread adoption.[75] As one participant stated, "promoting privacy and data protection principles remains paramount to ensure societal acceptance of IoT services."[76]

[73] *See* Dario Carluccio & Stephan Brinkhaus, Presentation: "Smart Hacking for Privacy," 28th Chaos Communication Congress, Berlin, December 2011, *available at* https://www.youtube.com/watch?v=YYe4SwQn2GE&feature=youtu.be. Moreover, "the two-second reporting interval provides so much data that [the researchers] were able to accurately chart power usage spikes and lulls indicative of times a homeowner would be home, asleep or away." *Id.* (In most smart meter implementations, data is reported at much longer intervals, usually fifteen minutes.) In addition to the privacy concerns, as noted above, the researchers discovered that the encryption was not implemented properly and that they could alter the energy consumption data reported by the meter. *Id.*

[74] *See, e.g.*, Fink & Segall, *supra* note 42 (describing a security vulnerability in Samsung smart TVs, since patched, that "enabled hackers to remotely turn on the TVs' built-in cameras without leaving any trace of it on the screen").

[75] *See, e.g.*, *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 17-18; *Comment of CTIA – The Wireless Ass'n*, #510 cmt. #00014 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5.

[76] *Comment of GS1 US*, #484 cmt. #00030 at 4.

Application of Traditional Privacy Principles

Summary of Workshop Discussions

Participants debated how the long-standing Fair Information Practice Principles ("FIPPs") of notice, choice, access, accuracy, data minimization, security, and accountability should apply to the IoT space. While some participants continued to support the application of all of the FIPPs,[77] others argued that data minimization, notice, and choice are less suitable for protecting consumer privacy in the IoT.[78]

The FIPPs were first articulated in 1973 in a report by what was then the U.S. Department of Health, Education and Welfare.[79] Subsequently, in 1980, the Organization for Economic Cooperation and Development ("OECD") adopted a set of privacy guidelines, which embodied the FIPPs.[80] Over time, the FIPPs have formed the basis for a variety of both government and private sector initiatives on privacy. For example, both the European Union

[77] *See, e.g.*, Remarks of Michelle Chibba, Office of the Information and Privacy Commissioner, Ontario, Canada ("Chibba"), Transcript of Workshop at 329; Remarks of Jacobs, Transcript of Workshop at 328-329; *Comment of AAA*, #510 cmt. #00012 at 2; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3.

[78] *See, e.g.*, *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3.

[79] *See* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 48 n.27 (1998), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[80] *See* OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. (In 2013, the OECD updated its guidelines to address risk management, interoperability, and other issues. The update is available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf). *See also* FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 3-4, 43 n.25 (2000).

Directive on the protection of personal data[81] and the Health Insurance Portability and Accountability Act ("HIPAA")[82] are based, in large part, on the FIPPs. In addition, many self-regulatory guidelines include the principles of notice, choice, access, and security.[83] The Obama Administration's Consumer Privacy Bill of Rights also includes these principles,[84] as does the privacy framework set forth in the Commission's 2012 Privacy Report.[85]

Workshop discussion focused on four FIPPs in particular – data security, data minimization, notice, and choice. As to data security, there was widespread agreement on the need for companies manufacturing IoT devices to incorporate reasonable security into these devices. As one participant stated, "Inadequate security presents the greatest risk of actual consumer harm in the Internet of Things."[86] Accordingly, as another participant noted,

---

[81] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[82] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[83] *See, e.g.*, NETWORK ADVER. INITIATIVE, NAI CODE OF CONDUCT 2013, *available at* http://www.networkadvertising.org/2013_Principles.pdf; INTERNET ADVER. BUREAU, INTERACTIVE ADVERTISING PRIVACY PRINCIPLES (Feb. 24, 2008), *available at* http://www.iab.net/guidelines/508676/1464.

[84] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[85] FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS vii-viii (2012) ("Privacy Report"), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. Commissioners Ohlhausen and Wright were not members of the Commission at that time and thus did not offer any opinion on that matter.

[86] *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 9 (and listing types of security measures that are already being implemented to secure the IoT).

"[s]ecurity must be built into devices and networks to prevent harm and build consumer trust in the IoT." [87]

Participants were more divided about the continuing applicability of the principles of data minimization, notice, and choice to the IoT.[88] With respect to data minimization – which refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it – one participant expressed concerns that requiring fledgling companies to predict what data they should minimize would "chok[e] off potential benefits and innovation."[89] A second participant cautioned that "[r]estricting data collection with rules like data minimization could severely limit the potential opportunities of the Internet of Things" based on beneficial uses that could be found for previously-collected data that were not contemplated at the time of collection.[90] Still another participant noted that "[d]ata-driven innovation, in many ways, challenges many interpretations of data minimization where data purpose specification and use limitation are overly rigid or prescriptive."[91]

With respect to notice and choice, some participants expressed concern about its feasibility, given the ubiquity of IoT devices and the persistent and pervasive nature of the

---

[87] *Comment of Infineon Tech. N. Am. Corp.*, #510 cmt. #00009 at 2; *see also* Remarks of Rogers, Transcript of Workshop at 312 ("There are some pretty good examples out there of what happens to companies when security becomes an afterthought and the cost that companies can incur in trying to fight the damage, the cost to brand reputation, the loss of customer confidence. And there are also some great examples of companies, even in the Internet of Things, as new as it is, companies that have gotten it right and they've done well. And they've gone on to push out products where there have been no issues.").

[88] *See, e.g.*, *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3-4.

[89] Remarks of Dan Caprio, McKenna, Long & Aldridge, LLP ("Caprio"), Transcript of Workshop at 339.

[90] *Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 3.

[91] *Comment of Software & Info. Indus. Ass'n*, #484 cmt. #00025 at 6–7; *see also Comment of Future of Privacy Forum*, #510 cmt. #00013 at 5 (purpose specification and data minimization as applied to the IoT "risks unduly limiting the development of new services and the discoveries that may follow from valuable research").

information collection that they make possible. As one participant observed, when "a bunch of different sensors on a bunch of different devices, on your home, your car, your body . . . are measuring all sorts of things," it would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported.[92] Another participant talked about the risk that, if patients have "to consent to everything" for a health monitoring app, "patients will throw the bloody thing away."[93] Yet another participant noted that any requirement to obtain consent could be "a barrier to socially beneficial uses of information."[94]

A related concern is that many IoT devices – such as home appliances or medical devices – have no screen or other interface to communicate with the consumer, thereby making notice on the device itself difficult, if not impossible.[95] For those devices that do have screens, the screens may be smaller than even the screens on mobile devices, where providing notice is already a challenge.[96] Finally, even if a device has screens, IoT sensors may collect data at times when the consumer may not be able to read a notice (for example, while driving).[97]

---

[92] Remarks of Peppet, Transcript of Workshop at 215–16.

[93] Remarks of Iyer, Transcript of Workshop at 230.

[94] *Comment of Software & Info. Indus. Ass'n*, #484 cmt. #00025 at 8.

[95] *See, e.g., Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 2 and 6; *Comment of Transatl. Computing Continuum Policy Alliance*, #510 cmt. #00017 at 2.

[96] *See* FTC STAFF REPORT, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 10–11 (2013) ("Mobile Disclosures Report"), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[97] In addition, some participants also suggested that notice and choice is not workable for IoT products and services that are not consumer-facing – *e.g.*, a sensor network to monitor electricity use in hotels. *See, e.g.*, *Comment of GS1 US*, #484 cmt. #00030 at 5 (noting that "[i]t is difficult to anticipate how the existing mechanisms of notice and choice, both being sound principles for privacy protection, would apply to sensors. . . . [H]ow would one provide adequate notice for every embedded sensor network? How would consent be obtained?"); *Comment of Future of*

Despite these challenges, participants discussed how companies can provide data minimization, notice, and choice within the IoT. One participant suggested that, as part of a data minimization exercise, companies should ask themselves a series of questions, such as whether they need a particular piece of data or whether the data can be deidentified.[98] Another participant gave a specific example of how data could be minimized in the context of connected cars. This participant noted that the recording device on such cars could "automatically delete old data after a certain amount of time, or prevent individual data from being automatically synched with a central database."[99]

As to notice and choice, one auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in "[p]lain language and multiple choices of levels."[100] Another discussed a "consumer profile management portal[]" approach that would include privacy settings menus that consumers can configure and revisit,[101] possibly on a separate device such as a smartphone or a webportal. In addition to the types of specific settings and choices, another participant suggested that devices and their associated platforms could enable consumers to aggregate choices into "packets."[102] Finally, one participant noted that

---

Privacy Forum, #510 cmt. #00013, Appendix A at 4. As noted above, this report addresses privacy and security practices for consumer-facing products.

[98] Remarks of Chibba, Transcript of Workshop at 300-01.

[99] Comment of EPIC, #484 cmt. #00011 at 17-18.

[100] Remarks of Kenneth Wayne Powell, Toyota Technical Center ("Powell"), Transcript of Workshop at 278.

[101] *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

[102] Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology ("Hall"), Transcript of Workshop at 216.

companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize privacy choices.[103]

Some participants advocated for an increased focus on certain types of use restrictions to protect consumer data.[104] With this approach, legislators, regulators, self-regulatory bodies, or individual companies would set "permissible" and "impermissible" uses of certain consumer data. One commenter characterized this approach as "shifting responsibility away from data subjects toward data users, and increasing the emphasis on responsible data stewardship and accountability."[105]

Participants offered a variety of approaches to adding use-based data protections. One participant proposed that companies "tag" data with its appropriate uses so that automated processes could identify and flag inappropriate uses.[106] Other participants noted that policymakers could constrain certain uses of IoT data that do not comport with consumer expectations and present the most risk of harm, either through law[107] or through voluntary

[103] Remarks of Nguyen, Transcript of Workshop at 48.

[104] *See* Remarks of Peppet, Transcript of Workshop at 210-211 (advocating "drawing some lines around acceptable use" through legislation or regulation in addition to notice and choice); *see also* Remarks of Crosley at 213 (supporting "the appropriate use of the context"); Remarks of Hall at 214 (expressing support for "[u]se restrictions, as long as they have teeth. That's why I think vanilla self-regulatory efforts are probably not the answer. You need to have something that is enforced by an independent body").

[105] Comment of Software & Information Industry Association, #484 cmt #00025 at 8.

[106] *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 10–11 (citing Hal Abelson, *Information Accountability as the Foundation of 21st Century Privacy Protection* (2013), *available at* http://kit.mit.edu/sites/default/files/documents/Abelson_MIT_KIT_2013_Conference.pdf). We note that such an approach would require coordination and potential associated costs.

[107] *See* Peppet, *Regulating the Internet of Things*, *supra* note 62, at 149 (proposing regulatory constraints).

self-regulatory efforts[108] or seal programs.[109] For example, as one participant has pointed out, some state laws restrict access by auto insurance companies and other entities to consumers' driving data recorded by an EDR.[110]

Post-Workshop Developments

Since the November 2013 workshop, the IoT marketplace has continued to develop at a remarkable pace. For example, in June 2014, Apple announced "HealthKit," a platform that "functions as a dashboard for a number of critical metrics as well as a hub for select third-party fitness products,"[111] as a way to help protect health information that some connected devices may collect. Similarly, in October 2014, Microsoft announced Microsoft Health, a "cloud-based service that … provid[es] actionable insights based on data gathered from the fitness devices and apps" and which will work in conjunction with Microsoft's HealthVault, which for a decade has offered "a trusted place to store health information and share it with medical professionals on a security-enhanced platform."[112] And last November, Intel announced a "new platform …

[108] *See, e.g.*, *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 7; *Comment of Direct Mktg. Ass'n*, #484 cmt. #00010 at 2; *Comment of CTIA – The Wireless Ass'n*, # 510 cmt. #00014 at 4; *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

[109] *See, e.g.*¸*Comment of AT&T Inc.*, #484 cmt. #00004 at 9–10; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 13.

[110] Peppet, *Regulating the Internet of Things*, *supra* note 62, at 153-54.

[111] Rachel King, *Apple takes app-based approach to health tech with HealthKit*, ZDNet (June 2, 2014), *available at* http://www.zdnet.com/article/apple-takes-app-based-approach-to-health-tech-with-healthkit/.

[112] Microsoft Health, http://www.microsoft.com/Microsoft-Health/en-us (last visited Jan. 9, 2015).

designed to make it easier for developers to connect devices securely, bring device data to the cloud, and make sense of that data with analytics."[113]

Policymakers have also tried to keep pace with these developments in the IoT. For example, in May 2014, the White House released a Big Data report ("White House Big Data Report"), and the President's Council of Advisors on Science and Technology released a companion report ("PCAST Report"). Both reports weigh in on the debate between the application of data minimization, notice, and choice versus use limitations. The White House Big Data Report opined that "the notice and consent framework threatens to be overcome" in certain instances, "such as the collection of ambient data by our household appliances."[114] The White House Big Data Report concluded that,

> Putting greater emphasis on a responsible use framework has many potential advantages. It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.[115]

Attention to the impact of the IoT spans the globe. In September 2014, Europe's Article 29 Working Group – composed of data protection authorities of EU member countries – issued

---

[113] Aaron Tilley, Intel Releases New Platform To Kickstart Development In The Internet Of Things, FORBES (Dec. 9, 2014), *available at* http://www.forbes.com/sites/aarontilley/2014/12/09/intel-releases-new-platform-to-kickstart-development-in-the-internet-of-things/.

[114] Executive Office of the President, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (May 2014) ("White House Big Data Report") at 56, *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. *See also* President's Council of Advisors on Science and Technology, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (May 2014), *available at* http://www.whitehouse.gov/administration/eop/ostp/pcast.

[115] *White House Big Data Report* at 56.

an Opinion on Recent Developments on the Internet of Things.[116] In the opinion, the Working Group emphasized the importance of user choice, noting that "users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific."

In addition to policy work by government agencies, standards organizations related to the Internet of Things continue to proliferate. One such area for standard-setting is data security. For example, in August 2014, oneM2M, a global standards body, released a proposed security standard for IoT devices. The standard addresses issues such as authentication, identity management, and access control.[117]

Commission Staff's Views and Recommendations for Best Practices

This section sets forth the Commission staff's views on the issues of data security, data minimization, and notice and choice with respect to the IoT and provides recommendations for best practices for companies.

DATA SECURITY

As noted, there appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Participants also discussed a number of specific security best practices. The Commission staff encourages companies to consider adopting these

[116] Article 29 Working Group Opinion, *supra* note 55.

[117] *See* oneM2M, *Technical Specification*, *oneM2M Security Solutions* at 15-16, *available at* http://www.onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf.

practices. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities. Nonetheless, the specific security best practices companies should consider include the following:

First, companies should implement "security by design" by building security into their devices at the outset, rather than as an afterthought.[118] One participant stated that security should be designed into every IoT product, at every stage of development, including "early on in the design cycle of a technology."[119] In addition, a company should do a privacy or security risk assessment, consciously considering the risks presented by the collection and retention of consumer information.[120] As part of this process, companies should incorporate the use of smart defaults, such as requiring consumers to change default passwords – if they use default passwords at all – during the set-up process.[121] Companies also should consider how to minimize the data they collect and retain, as discussed further below. Finally, companies should test their security measures before launching their products. As one participant pointed out, such testing should occur because companies – and service providers they might use to help develop their

[118] *Comment of ARM and AMD*, #510 cmt. #00018 at 2; *see also* Remarks of Hagins, Transcript of Workshop at 111; Remarks of Jacobs, Transcript of Workshop at 296; Remarks of Caprio, Transcript of Workshop at 298.

[119] Remarks of Kohno, Transcript of Workshop at 281.

[120] Remarks of Chibba, Transcript of Workshop at 301; *see also* Remarks of Rogers, Transcript of Workshop at 343.

[121] *See generally* Remarks of Rogers, Transcript of Workshop at 344 ("Default passwords are something that should never pass through into production space. It's an easy thing to pick up with a very basic assessment, yet we are constantly seeing these come through because these companies aren't often doing this kind of assessment − so they see it as a hindrance, an extra step. Or they claim the consumer should be responsible for setting the security, once it lands on the consumer's desk which, at the end of the day, the consumers aren't capable of setting that level of security, nor should they have to.").

products – may simply forget to close "backdoors" in their products through which intruders could access personal information or gain control of the device.[122]

This last point was illustrated by the Commission's recent actions against the operators of the Credit Karma and Fandango mobile apps. In these cases, the companies overrode the settings provided by the Android and iOS operating systems, so that SSL encryption was not properly implemented. As a result, the Commission alleged, hackers could decrypt the sensitive consumer financial information being transmitted by the apps. The orders in both cases include provisions requiring the companies to implement reasonable security.[123]

Second, companies must ensure that their personnel practices promote good security. As part of their personnel practices, companies should ensure that product security is addressed at the appropriate level of responsibility within the organization. One participant suggested that "if someone at an executive level has responsibility for security, it tends to drive hiring and processes and mechanisms throughout the entire organization that will improve security."[124] Companies should also train their employees about good security practices, recognizing that technological expertise does not necessarily equate to security expertise. Indeed, one participant stated that being able to write software code "doesn't mean…understand[ing] anything whatsoever about the security of an embedded device."[125]

---

[122] *See generally* Remarks of Heffner, Transcript of Workshop at 73-74.

[123] Credit Karma, Inc., File No. 132-3091 (Mar. 28, 2014) (consent), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc; Fandango, LLC, File No. 132-3089 (Mar. 28, 2014) (consent), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc. *See also* HTC America, Inc., No. C-4406 (July 2, 2013) (consent) (alleging that HTC, among other things, failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter.

[124] Remarks of Hagins, Transcript of Workshop at 110.

[125] *Id.* at 92.

Third, companies must work to ensure that they retain service providers that are capable of maintaining reasonable security, and provide reasonable oversight to ensure that those service providers do so. Failure to do so could result in an FTC law enforcement action. For example, in the Commission's recent settlement with GMR Transcription Services, the Commission alleged that a medical and legal transcription company outsourced transcription services to independent typists in India without adequately checking to make sure they could implement reasonable security measures. According to the Commission's complaint, among other things, the service provider stored transcribed notes in clear text on an unsecured server. As a result, U.S. consumers found their doctors' notes of their physical examinations freely available through Internet searches. This case illustrates the strong need for appropriate service provider oversight.

Fourth, for systems with significant risk, companies should implement a defense-in-depth approach, where security measures are considered at several levels. For example, participants raised concerns about relying on the security of consumers' own networks, such as passwords for their Wi-Fi routers, alone to protect the information on connected devices.[126] They noted that companies must take "additional steps to encrypt [the information] or otherwise secure it."[127] FTC staff shares these concerns and encourages companies to take additional steps to secure information passed over consumers' home networks. Indeed, encryption for sensitive information, such as that relating to health, is particularly important in this regard.[128] Regardless of the specific technology, companies should reasonably secure data in transit and in storage.

[126] *Id.* at 102.

[127] Remarks of Heffner, Transcript of Workshop at 102-03.

[128] Remarks of Hall, Transcript of Workshop at 178-79.

Fifth, panelists noted that companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network.[129] In the IoT ecosystem, strong authentication could be used to permit or restrict IoT devices from interacting with other devices or systems. The privileges associated with the validated identity determine the permissible interactions between the IoT devices and could prevent unauthorized access and interactions.[130] In implementing these protections, companies should ensure that they do not unduly impede the usability of the device. As noted above, the proposed oneM2M security standard includes many of the recommendations discussed above.[131] Such efforts are important to the success of IoT.

Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities. Many IoT devices have a limited life cycle, resulting in a risk that consumers will be left with out-of-date IoT devices that are vulnerable to critical, publicly known security or privacy bugs. Companies may reasonably decide to limit the time during which they provide security updates and software patches, but it is important that companies weigh these decisions carefully. Companies should also be forthright in their representations about providing ongoing security updates and software patches. Disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the safe 'expiration dates' for their commodity Internet-

---

[129] *See, e.g.*, BRETT C. TJADEN, FUNDAMENTALS OF SECURE COMPUTER SYSTEMS 5 (2004). *See also* HP, INTERNET OF THINGS RESEARCH STUDY, *supra* note 41, at 4-5 (noting that approximately 60% of IoT devices examined had weak credentials).

[130] There may be other appropriate measures, as the security measures that a company should implement vary, depending on the risks presented by unauthorized access to the device, and the sensitivity of any information collected.

[131] oneM2M Candidate Release August 2014, *available at* http://www.onem2m.org/technical/candidate-release-august-2014 (last visited Dec. 19, 2014).

connected devices. In addition, companies that do provide ongoing support should also notify consumers of security risks and updates.

Several of these principles are illustrated by the Commission's first case involving an Internet-connected device. TRENDnet[132] marketed its Internet-connected cameras for purposes ranging from home security to baby monitoring, claiming that they were "secure." In its complaint, the Commission alleged, among other things, that the company transmitted user login credentials in clear text over the Internet, stored login credentials in clear text on users' mobile devices, and failed to test consumers' privacy settings to ensure that video feeds marked as "private" would in fact be private.[133] As a result of these alleged failures, hackers were able to access live feeds from consumers' security cameras and conduct "unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."[134] This case demonstrates the importance of practicing security-by-design.

[132] Press Release, FTC, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

[133] Complaint of FTC, TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (consent), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[134] *Id*. at 5.

Of course, the IoT encompasses a wide variety of products and services, and, as noted, the specific security measures that a company needs to implement will depend on a number of factors.[135] Devices that collect sensitive information, present physical security or safety risks (such as door locks, ovens, or insulin pumps), or connect to other devices or networks in a manner that would enable intruders to access those devices or networks should be more robustly secured than, for example, devices that simply monitor room temperatures, miles run, or calories ingested.

DATA MINIMIZATION

Commission staff agrees with workshop participants who stated that the data minimization principle remains relevant and important to the IoT.[136] While staff recognizes that companies need flexibility to innovate around new uses of data, staff believes that these interests can and should be balanced with the interests in limiting the privacy and data security risks to consumers.[137] Accordingly, companies should examine their data practices and business needs

[135] *See, e.g.*, FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf:

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

[136] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7.

[137] *See, e.g.*, *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3; Remarks of Chibba, Transcript of Workshop at 329–30.

and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.[138]

Data minimization is a long-standing principle of privacy protection and has been included in several policy initiatives, including the 1980 OECD Privacy Guidelines, the 2002 Asia-Pacific Economic Cooperation ("APEC") Privacy Principles, and the 2012 White House Consumer Privacy Bill of Rights.[139] Some observers have debated how data minimization would apply to new technologies.[140] In the IoT ecosystem, data minimization is challenging, but it remains important.[141] Indeed, data minimization can help guard against two privacy-related risks. First, collecting and retaining large amounts of data increases the potential harms associated with a data breach, both with respect to data stored on the device itself as well as in the cloud. Larger data stores present a more attractive target for data thieves, both outside and inside a company –

---

[138] Privacy Report, *supra* note 85, at 26–27; *see also* Mobile Disclosures Report, *supra* note 96, at 1 n.2; FTC, Data Brokers: A Call for Transparency and Accountability 55 (2014) ("Data Broker Report"), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[139] *See* Privacy Report, *supra* note 85, at 26–27; OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, at ¶ 7 (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (same); Dept. of Homeland Security, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security § 5 (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (stating a Data Minimization principle: "DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)."); Exec. Office of the President, National Strategy for Trusted Identities in Cyberspace 45 (Apr. 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (stating a Data Minimization principle: "Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).").

[140] *See* White House Big Data Report, *supra* note 114, at 54 (Because "the logic of collecting as much data as possible is strong … focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy."); PCAST Report at x-xi ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).").

[141] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7. *See also* Article 29 Working Group Opinion, *supra* note 55, at 16–17.

and increases the potential harm from such an event.[142] Thieves cannot steal data that has been deleted after serving its purpose; nor can thieves steal data that was not collected in the first place. Indeed, in several of its data security cases, the Commission has alleged that companies could have mitigated the harm associated with a data breach by disposing of customer information they no longer had a business need to keep.[143]

Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations. For example, in 2010, Commission staff sent a letter to the founders of XY magazine, a magazine for gay youth, regarding their negotiations to sell in bankruptcy customer information dating back to as early as 1996. The staff noted that, because the magazine had ceased to exist for a period of three years, the subscribers were likely to have become adults and moved on, and because continued use of their information would have been contrary to their reasonable expectations, XY should delete the personal information.[144] In this case, the risk associated with continued storage and use of the subscribers' personal information contrary to their reasonable expectations would not have existed if the company had engaged in reasonable data minimization practices.

Although these examples are not IoT-specific, they demonstrate the type of risk created by the expansive collection and retention of data. To minimize these risks, companies should

---

[142] Remarks of Chibba, Transcript of Workshop at 340; Privacy Report, *supra* note 85, at 27–29.

[143] *See CardSystems Solutions, Inc.*, No. C-4168, 2006 WL 2709787 (F.T.C. Sept. 5, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch; *DSW, Inc.*, No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006) (consent order); *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter. Commissioner Ohlhausen was not a commissioner at the time of these cases and therefore did not participate in them.

[144] Letter from David C. Vladeck, Dir., FTC Bureau of Consumer Prot., to Peter Larson and Martin E. Shmagin (July 1, 2010), *available at* http://www.ftc.gov/enforcement/cases-proceedings/closing-letters/letter-xy-magazine-xycom-regarding-use-sale-or.

examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.[145] Such an exercise is integral to a privacy-by-design approach and helps ensure that the company has given thought to its data collection practices on the front end by asking questions such as what types of data it is collecting, to what end, and how long it should be stored.[146] The process of mindfully considering data collection and retention policies and engaging in a data minimization exercise could also serve an education function for companies, while at the same time, protecting consumer privacy.[147]

As an example of how data minimization might work in practice, suppose a wearable device, such as a patch, can assess a consumer's skin condition. The device does not need to collect precise geolocation information in order to work; however, the device manufacturer believes that such information might be useful for a future product feature that would enable users to find treatment options in their area. As part of a data minimization exercise, the company should consider whether it should wait to collect geolocation until after it begins to offer the new product feature, at which time it could disclose the new collection and seek consent. The company should also consider whether it could offer the same feature while collecting less information, such as by collecting zip code rather than precise geolocation. If the company does decide it needs the precise geolocation information, it should provide a prominent disclosure about its collection and use of this information, and obtain consumers' affirmative

[145] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

[146] *Id. See also* Remarks of Chibba, Transcript of Workshop at 330.

[147] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

express consent. Finally, it should establish reasonable retention limits for the data it does collect.

To the extent that companies decide they need to collect and maintain data to satisfy a business purpose, they should also consider whether they can do so while maintaining data in de-identified form. This may be a viable option in some contexts and helps minimize the individualized data companies have about consumers, and thus any potential consumer harm, while promoting beneficial societal uses of the information. For example, one university hospital offers a website and an associated smart phone app that collect information from consumers, including geolocation information, to enable users to find and report flu activity in their area.[148] The hospital can maintain and post information in anonymous and aggregate form, which can benefit public health authorities and the public, while at the same time maintaining consumer privacy.

A key to effective de-identification is to ensure that the data cannot be reasonably re-identified. For example, U.S. Department of Health and Human Service regulations[149] require entities covered by HIPAA to either remove certain identifiers, such as date of birth and five-digit zip code, from protected health information[150] or have an expert determine that the risk of re-identification is "very small."[151] As one participant discussed,[152] in 2009, a group of experts attempted to re-identify approximately 15,000 patient records that had been de-identified under

[148] *See* Flu Near You, *available at* https://flunearyou.org/.

[149] 45 C.F.R. §§ 164.514(a)-(c).

[150] 45 C.F.R. § 165.514(b)(2).

[151] 45 C.F.R. § 165.514(b)(1).

[152] *Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 8.

the HIPAA standard. They used commercial data sources to re-identify the data and were able to identify only 0.013% of the individuals.[153] While deidentification can be challenging in several contexts,[154] appropriately de-identified data sets that are kept securely and accompanied by strong accountability mechanisms, can reduce many privacy risks.

Of course, as technology improves, there is always a possibility that purportedly de-identified data could be re-identified.[155] This is why it is also important for companies to have accountability mechanisms in place. When a company states that it maintains de-identified or anonymous data, the Commission has stated that companies should (1) take reasonable steps to de-identify the data, including by keeping up with technological developments; (2) publicly commit not to re-identify the data; and (3) have enforceable contracts in place with any third parties with whom they share the data, requiring the third parties to commit not to re-identify the data.[156] This approach ensures that if the data is not reasonably de-identified and then is re-identified in the future, regulators can hold the company responsible.

With these recommendations on data minimization, Commission staff is mindful of the need to balance future, beneficial uses of data with privacy protection. For this reason, staff's recommendation is a flexible one that gives companies many options: they can decide not to

---

[153] *Id.*

[154] Technical experts continue to evaluate the effectiveness of deidentification for different types of data, and some urge caution in interpreting claims about the effectiveness of specific technical means of deidentification. *See, e.g.*, Arvind Narayanan and Edward Felten, No Silver Bullet: De-Identification Still Doesn't Work (July 9, 2014), *available at* http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf.

[155] *See, e.g.*, Ann Cavoukian and Khaled El Emam, De-identification Protocols: Essential for Protecting Privacy (June 25, 2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identifcation_essential.pdf; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 8; Privacy Report, *supra* note 85, at 21.

[156] *See* Privacy Report, *supra* note 85, at 21; *see also Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 7.

collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options work, it can seek consumers' consent for collecting additional, unexpected data. In addition, in considering reasonable collection and retention limits, it is appropriate to consider the sensitivity of the data at issue: the more sensitive the data, the more harmful it could be if the data fell into the wrong hands or were used for purposes the consumer would not expect. Through this approach, a company can minimize its data collection, consistent with its business goals.[157] As one participant noted, "[p]rotecting privacy and enabling innovation are not mutually exclusive and must consider principles of accountability and privacy by design."[158]

NOTICE AND CHOICE

While the traditional methods of providing consumers with disclosures and choices may need to be modified as new business models continue to emerge, staff believes that providing notice and choice remains important, as potential privacy and security risks may be heightened due to the pervasiveness of data collection inherent in the IoT. Notice and choice is particularly important when sensitive data is collected.[159]

---

[157] *See, e.g.*, *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 10 (describing its Smart Grid privacy seal).

[158] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 3. *See also* Remarks of Chibba, Transcript of Workshop at 330.

[159] *See, e.g.*, *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 6 ("In some cases, however, such as when consumers are purchasing connected devices that will collect personally identifiable health information, the presentation of privacy policies will be important to helping consumers make informed choices."); *Comment of Ctr. for Digital Democracy*, #484 cmt. #00006 at 3 ("[T]he combined impact of the mobile marketing and real-time data revolution and the Internet of Things places consumer privacy at greater risk than ever before.").

Moreover, staff believes that providing consumers with the ability to make informed choices remains practicable in the IoT. This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits.[160] This principle applies equally to the Internet of Things.

For example, suppose a consumer buys a smart oven from ABC Vending, which is connected to an ABC Vending app that allows the consumer to remotely turn the oven on to the setting, "Bake at 400 degrees for one hour." If ABC Vending decides to use the consumer's oven-usage information to improve the sensitivity of its temperature sensor or to recommend another of its products to the consumer, it need not offer the consumer a choice for these uses, which are consistent with its relationship with the consumer. On the other hand, if the oven manufacturer shares a consumer's personal data with, for example, a data broker or an ad network, such sharing would be inconsistent with the context of the consumer's relationship with the manufacturer, and the company should give the consumer a choice. The practice of distinguishing contextually appropriate data practices from those that are inconsistent with

[160] Privacy Report, *supra* note 85, at 38-39; *id.* at 38 ("The Commission believes that for some practices, the benefits of providing choice are reduced – either because consent can be inferred or because public policy makes choice unnecessary.").

context reduces the need for companies to provide opportunities for consumer choice before every single data collection.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface, and recognizes that there is no one-size-fits-all approach. Some options – several of which were discussed by workshop participants – include the following:

- **Choices at point of sale:**
  One auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in "[p]lain language and multiple choices of levels."[161]

- **Tutorials:**
  Facebook offers a video tutorial to guide consumers through its privacy settings page. IoT device manufacturers can offer similar vehicles for explaining and providing choices to consumers.

- **Codes on the device:**
  Manufacturers could affix a QR code or similar barcode that, when scanned, would take the consumer to a website with information about the applicable data practices and enable consumers to make choices through the website interface.[162]

- **Choices during set-up:**
  Many IoT devices have an initial set-up wizard, through which companies could provide clear, prominent, and contextual privacy choices.

[161] Remarks of Kenneth Wayne Powell, Toyota Technical Center ("Powell"), Transcript of Workshop at 278.

[162] *See* Article 29 Working Group Opinion, *supra* note 55, at 18 (proposing that a "device manufacturer could print on things equipped with sensors a QR code, or a flashcode describing the type of sensors and the information it captures as well as the purposes of these data collections").

- **Management portals or dashboards:**[163]
  In addition to the availability of initial set-up choices, IoT devices could also include privacy settings menus that consumers can configure and revisit. For example, in the mobile context, both Apple and Google (for Android) have developed dashboard approaches that seem promising – one that is framed by data elements, such as geolocation and contacts (Apple), and one that is framed by individual apps (Android).[164] Similarly, companies developing "command centers" for their connected home devices[165] could incorporate similar privacy dashboards. Properly implemented, such "dashboard" approaches can allow consumers clear ways to determine what information they agree to share.

- **Icons:**
  Devices can use icons to quickly convey important settings and attributes, such as when a device is connected to the Internet, with a toggle for turning the connection on or off.

- **"Out of Band" communications requested by consumers:**
  When display or user attention is limited, it is possible to communicate important privacy and security settings to the user via other channels. For example, some home appliances allow users to configure their devices so that they receive important information through emails or texts.

- **General Privacy Menus:**
  In addition to the types of specific settings and choices described above, devices and their associated platforms could enable consumers to aggregate choices into "packets." [166] This could involve having more general settings like "low privacy," "medium," or "high," accompanied by a clear and conspicuous explanation of the settings.

- **A User Experience Approach:**
  One participant noted that companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize choices.[167] For example, a manufacturer that offers two or more devices could use the consumer's preferences on one device (*e.g.*, "do not transmit any of my information to third parties") to set a default preference on another. As another example, a single device, such as a home appliance "hub" that stores data locally – say on the consumer's home network – could learn a consumer's preferences based on prior behavior and predict future privacy preferences as new appliances are added to the hub.

---

[163] *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

[164] *See* Mobile Disclosures Report, *supra* note 96, at 16-17.

[165] Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL ST. J. (Jan. 4, 2015), *available at* http://www.wsj.com/articles/the-race-to-build-command-centers-for-smart-homes-1420399511.

[166] Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology ("Hall"), Transcript of Workshop at 216.

[167] Remarks of Nguyen, Transcript of Workshop at 48.

Of course, whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents.[168] In addition, companies may want to consider using a combination of approaches.

Staff also recognizes concerns discussed at the workshop[169] and, as noted above, in the White House Big Data Report and PCAST Report that, applied aggressively, a notice and choice approach could restrict unexpected new uses of data with potential societal benefits. For this reason, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. Companies should not collect sensitive data without affirmative express consent.

In addition, if a company enables the collection of consumers' data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. As noted above, robust de-identification measures can enable companies to analyze data they collect in order to innovate in a privacy-protective way.[170] Companies can use such de-identified data without having to offer consumers choices.

---

[168] This discussion refers to how companies should communicate choices to consumers. Lengthy privacy policies are not the most effective consumer communication tool. However, providing disclosures and choices through these privacy policies serves an important accountability function, so that regulators, advocacy groups, and some consumers can understand and compare company practices and educate the public. *See* Privacy Report, *supra* note 85, at 61-64.

[169] *See, e.g., Comment of Future of Privacy Forum*, #510 cmt. #00013, App. A at 9; *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 6-9.

[170] *See, e.g.*, Comment of CTIA – The Wireless Ass'n, #484 cmt. #00009 at 10-11; Comment of Future of Privacy Forum, #510 cmt. #00013 at 5.

Staff also notes that existing laws containing elements of the use-based approach apply to the IoT. The FCRA sets forth a number of statutory protections applicable to "consumer report" information, including restrictions on the uses for which this information can be shared.[171] Even when there is a permissible use for such information, the FCRA imposes an array of protections, including those relating to notice, access, disputes, and accuracy.[172] In addition, the FTC has used its "unfairness" authority to challenge a number of harmful uses of consumer data. For example, in the agency's recent case against Leap Lab, the Commission alleged that defendants sold consumer payday loan applications that included consumers' Social Security and financial account numbers to non-lenders that had no legitimate need for this sensitive personal information.[173]

Staff has concerns, however, about adopting solely a use-based model for the Internet of Things. First, because use-based limitations have not been fully articulated in legislation or other widely-accepted multistakeholder codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful.[174] If a company decides that a particular data use is beneficial and consumers disagree with that decision, this may erode consumer trust. For example, there was considerable consumer outcry over Facebook's launch of the Beacon service,

---

[171] FCRA, 15 U.S.C. § 1681–1681v. Section 604 of the FCRA sets forth the permissible purposes for which a consumer reporting company may furnish consumer report information, such as to extend credit or insurance or for employment purposes. 15 U.S.C. 1681b.

[172] FCRA, 15 U.S.C. § 1681–1681v.

[173] Press Release, FTC, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts (Dec. 23, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars.

[174] ANN CAVOUKIAN ET AL., INFO. & PRIVACY COMM'R, ONT., CAN., THE UNINTENDED CONSEQUENCES OF PRIVACY PATERNALISM (2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/03/pbd-privacy_paternalism.pdf.

as well as Google's launch of the Buzz social network, which ultimately led to an FTC enforcement action.[175]

Second, use limitations alone do not address the privacy and security risks created by expansive data collection and retention. As explained above, keeping vast amounts of data can increase a company's attractiveness as a data breach target, as well as the risk of harm associated with any such data breach. For this reason, staff believes that companies should seek to reasonably limit the data they collect and dispose of it when it is no longer needed.

Finally, a use-based model would not take into account concerns about the practice of collecting sensitive information.[176] Consumers would likely want to know, for example, if a company is collecting health information or making inferences about their health conditions, even if the company ultimately does not use the information.[177]

---

[175] *See, e.g.*, Google Inc., No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

[176] In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

[177] Of course, if a company misstates how it uses data, this could be a deceptive practice under Section 5 of the FTC Act. The FTC has brought cases against companies that promise to use consumers' data one way, but used it in another way. *See, e.g.*, Google Inc., *supra* note 175. The FTC can also use its unfairness authority to prohibit uses of data that cause or are likely to cause substantial injury to a consumer, where that injury was not reasonably avoidable by the consumer, and where the injury was not outweighed by a benefit to consumers or competition. *See, e.g.*, Designerware, LLC, No. C-4390 (Apr. 11, 2013) (consent order) (alleging that installing and turning on webcams on people's home computers without their knowledge or consent was an unfair practice), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter.

The establishment of legislative or widely-accepted multistakeholder use-based frameworks could potentially address some of these concerns and should be considered. For example, the framework could set forth permitted or prohibited uses. In the absence of such legislative or widely accepted multistakeholder frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

Legislation

Summary of Workshop Discussions

Workshop participants discussed whether legislation is needed to ensure appropriate protections for data collected through connected devices. Some participants expressed trepidation that the benefits of the IoT might be adversely affected should policymakers enact laws or regulations on industry.[178] One participant stated, "[t]he FTC should be very cautious about proposing regulation of this sector, given its importance to innovation in America."[179] Another participant noted that "we should be careful to kind of strike a balance between guiding companies in the right direction and enforcing."[180] Still another worried that the workshop might "represent[] the beginning of a regulatory regime for a new set of information technologies that are still in their infancy" and advised policymakers to "exercise restraint and avoid the impulse to regulate before serious harms are demonstrated."[181] Another participant questioned what legislation would look like, given the difficulty of defining the contours of privacy rights.[182]

A number of participants noted that self-regulation is the appropriate approach to take to the IoT. One participant stated, "self-regulation and best business practices – that are technology

[178] *See, e.g.*, *Comment of Direct Mktg. Ass'n*, #484 cmt. #00010.

[179] *Comment of Internet Commerce Coal.*, #484 cmt. #00020 at 2.

[180] Remarks of Rogers, Transcript of Workshop at 359.

[181] *Comment of Tech. Policy Program of the Mercatus Ctr., George Mason Univ.*, #484 cmt. #00024 at 1 and 9.

[182] Remarks of Cerf, Transcript of Workshop at 149-50 ("Well, I have to tell you that regulation is tricky. And I don't know, if somebody asked me, would you write a regulation for this, I would not know what to say. I don't think I have enough understanding of all of the cases that might arise in order to say something useful about this, which is why I believe we are going to end up having to experience problems before we understand the nature of the problems and maybe even the nature of the solutions.").

neutral – along with consumer education serve as the preferred framework for protecting consumer privacy and security while enhancing innovation, investment, competition, and the free flow of information essential to the Internet of Things."[183] Another participant agreed, stating "[s]elf-regulatory regimes have worked well to ensure consumer privacy and foster innovation, and industry has a strong track record of developing and implementing best practices to protect information security."[184]

Other participants noted that the time is ripe for legislation, either specific to the IoT or more generally.[185] One participant who called for legislation noted that the "explosion of fitness and health monitoring devices is no doubt highly beneficial to public health and worth encouraging," but went on to state:

> At the same time, data from these Internet of Things devices should not be usable by insurers to set health, life, car, or other premiums. Nor should these data migrate into employment decisions, credit decisions, housing decisions, or other areas of public life. To aid the development of the Internet of Things—and reap the potential public health benefits these devices can create—we should reassure the public that their health data will not be used to draw unexpected inferences or incorporated into economic decisionmaking.[186]

Recommendations

The Commission staff recognizes that this industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees with those commenters who stated that there is

---

[183] *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

[184] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 18.

[185] Remarks of Hall, Transcript of Workshop at 180-81 (supporting baseline privacy legislation); *see also* Remarks of Jacobs, Transcript of Workshop at 360 (emphasizing importance of enforcement "in the meantime").

[186] Peppet, *Regulating the Internet of Things*, *supra* note 62, at 151.

great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature. Staff also agrees that development of self-regulatory programs[187] designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, while IoT specific-legislation is not needed, the workshop provided further evidence that Congress should enact general data security legislation. As noted above, there was wide agreement among workshop participants about the importance of securing Internet-enabled devices, with some participants stating that many devices now available in the market are not reasonably secure, posing risks to the information that they collect and transmit and also to information on consumers' networks or even to others on the Internet.[188] These problems highlight the need for substantive data security and breach notification legislation at the federal level.

The Commission has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach. Reasonable and appropriate security practices are critical to addressing the problem of data breaches and protecting consumers from identity theft and other harms. Notifying consumers of breaches after they occur helps consumers protect themselves from any harm that is likely to be caused by the misuse of their data. These principles apply equally to the IoT ecosystem.[189]

---

[187] Remarks of Lightner, Transcript of Workshop at 56-57 (discussing voluntary code of conduct for energy data); *Comment of Future of Privacy Forum*, #484 cmt. #00013 (discussing self-regulatory efforts in a variety of contexts).

[188] *See* discussion *supra* pp. 10-14 and accompanying notes.

[189] One commenter argued that breach notification laws should be even broader in the IoT context. *See* Remarks of Peppet, Transcript of Workshop at 220 (urging that breach notification laws be extended for the IoT to cover additional types of information that would lead to consumer harm but would not meet the definition of personal

We emphasize that general technology-neutral data security legislation should protect against unauthorized access to both personal information and device functionality itself. The security risks associated with IoT devices, which are often not limited to the compromise of personal information but also implicate broader health and safety concerns, illustrate the importance of these protections. For example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.[190] Similarly, a criminal who hacks into a car's network could cause a car crash. Accordingly, general data security legislation should address risks to both personal information and device functionality.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards.[191] Commission staff thus again recommends that Congress consider enacting broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as when to provide privacy notices to consumers and offer them choices about data collection and use practices. Although the Commission currently has authority to take action against some IoT-related practices, it cannot

---

information protected under existing laws). The Commission has not taken a position on such an approach at this time.

[190] Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/.

[191] Commissioner Ohlhausen disagrees with this portion of the staff's recommendation. She believes that the FTC's current Section 5 authority to prohibit unfair and deceptive acts or practices already requires notice and choice for collecting sensitive personally identifiable information and protects against uses of consumer information that cause or are likely to cause substantial consumer harm not outweighed by benefits to consumers or competition. Furthermore, the FCRA, HIPAA, and other laws already provide additional sector-specific privacy protections. Thus, Commissioner Ohlhausen questions what harms baseline privacy legislation would reach that the FTC's existing authority cannot.

mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness.

The Commission has issued a report and testified before Congress calling for baseline federal privacy legislation.[192] These recommendations have been based on concerns about the lack of transparency regarding some companies' data practices and the lack of meaningful consumer control of personal data. These concerns permeate the IoT space, given the ubiquity of information collection, the broad range of uses that the IoT makes possible, the multitude of companies involved in collecting and using information, and the sensitivity of some of the data at issue.

Staff believes such legislation will help build trust in new technologies that rely on consumer data, such as the IoT. Consumers are more likely to buy connected devices if they feel that their information is adequately protected.[193] A 2012 survey shows, for example, that a majority of consumers uninstalled an app because they were concerned that it was collecting too much personal information, or declined to install an app at all.[194] A 2014 survey shows that 87% of consumers are concerned about the type of data collected through smart devices, and 88% of

---

[192] *See, e.g.*, Privacy Report, *supra* note 85, at 12-13; *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. On Commerce, Science & Transportation* (May 9, 2012) (statement of FTC), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf.

[193] Remarks of Chibba, Transcript of Workshop at 312-13; *see also* Remarks of Wolf, Transcript of Workshop at 260 (noting that "the Michigan Department of Transportation and the Center for Automotive Research identified security as the primary concern for connected car technologies"); *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5 ("If there are lax controls and insufficient oversight over the collection of personal information through connected devices, consumers will lose trust in the evolving technologies. Even with proper controls and oversight, helping consumers understand the benefits from these innovations and the protections in place is important lest they feel that personal control has been sacrificed for corporate gain.").

[194] JAN LAUREN BOYLES ET AL., PEW INTERNET PROJECT, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (2012), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.

consumers want to control the data that is collected through smart devices.[195] Surveys also show that consumers are more likely to trust companies that provide them with transparency and choices.[196] General privacy legislation that provides for greater transparency and choices could help both consumers and businesses by promoting trust in the burgeoning IoT marketplace.

In addition, as demonstrated at the workshop, general privacy legislation could ensure that consumers' data is protected, regardless of who is asking for it. For example, workshop participants discussed the fact that HIPAA protects sensitive health information, such as medical diagnoses, names of medications, and health conditions, but only if it is collected by certain entities, such as a doctor's office or insurance company.[197] Increasingly, however, health apps are collecting this same information through consumer-facing products, to which HIPAA protections do not apply. Commission staff believes that consumers should have transparency and choices over their sensitive health information, regardless of who collects it. Consistent standards would also level the playing field for businesses.

---

[195] The TRUSTe Internet of Things Privacy Index, 2014 U.S. Edition, *available at* http://www.truste.com/us-internet-of-things-index-2014/.

[196] *See, e.g.*, Adam DeMartino, Evidon, *RESEARCH: Consumers Feel Better About Brands that Give Them Transparency and Control Over Ads* (Nov. 10, 2010), *available at* http://www.evidon.com/blog/research-consumers-feel-better-about-brands-that-give-them-transparency-and-control-over-ads; Scott Meyer, *Data Transparency Builds Trust*, BRANDREPUBLIC (Oct. 31, 2012), *available at* http://www.brandrepublic.com/news/1157134/; TRUSTe, *New TRUSTe Survey Finds Consumer Education and Transparency Vital for Sustainable Growth and Success of Online Behavioral Advertising* (July 25, 2011), *available at* http://www.truste.com/about-TRUSTe/press-room/news_truste_behavioral_advertising_survey_2011.

[197] Remarks of Hall, Transcript of Workshop at 179; Remarks of T. Drew Hickerson, Happtique, Transcript of Workshop at 350; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 12.

While Commission staff encourages Congress to consider privacy and security legislation, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices and services. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
  The Commission enforces the FTC Act, the FCRA, the Children's Online Privacy Protection Act, the health breach notification provisions of the HI-TECH Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws. The TRENDNet case, discussed above, was the Commission's first IoT case. We will continue to look for cases involving companies making IoT devices that, among other things, do not maintain reasonable security, make misrepresentations about their privacy practices, or violate the requirements of the FCRA when they use information for credit, employment, insurance, or other eligibility decisions. Staff believes that a strong FTC law enforcement presence will help incentivize appropriate privacy and security-protective practices by companies manufacturing and selling connected devices.

- **Consumer and business education:**
  Consumers should understand how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available privacy settings. Businesses, and in particular small businesses, would benefit from additional information about how to reasonably secure IoT devices. The Commission staff will develop new consumer and business education materials in this area.

- **Participation in multi-stakeholder groups:**
  Currently, Commission staff is working with a variety of groups that are considering guidelines related to the Internet of Things. For example, staff participates in NTIA's multi-stakeholder group that is considering guidelines for facial recognition and the Department of Energy's multi-stakeholder effort to develop guidelines for smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers. Commission staff will continue to participate in multistakeholder groups to develop guidelines related to the IoT.

- **Advocacy:**
  Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area. Among other things, staff will share the best practices discussed in this report with other government entities in order to ensure that they consider privacy and security issues.

Conclusion

The IoT presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car, and with wearables and ingestibles, even the body – poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation.

An Empirical Study of Web Vulnerability Discovery Ecosystems

Mingyi Zhao
Pennsylvania State University
muz127@ist.psu.edu

Jens Grossklags
Pennsylvania State University
jensg@ist.psu.edu

Peng Liu
Pennsylvania State University
pliu@ist.psu.edu

ABSTRACT

In recent years, many organizations have established bounty programs that attract white hat hackers who contribute vulnerability reports of web systems. In this paper, we collect publicly available data of two representative web vulnerability discovery ecosystems (Wooyun and HackerOne) and study their characteristics, trajectory, and impact. We find that both ecosystems include large and continuously growing white hat communities which have provided significant contributions to organizations from a wide range of business sectors. We also analyze vulnerability trends, response and resolve behaviors, and reward structures of participating organizations. Our analysis based on the HackerOne dataset reveals that a considerable number of organizations exhibit decreasing trends for reported web vulnerabilities. We further conduct a regression study which shows that monetary incentives have a significantly positive correlation with the number of vulnerabilities reported. Finally, we make recommendations aimed at increasing participation by white hats and organizations in such ecosystems.

Keywords

Bug Bounty; Vulnerability Discovery; Vulnerability Disclosure; Monetary Incentives

1. INTRODUCTION

Websites are critical pathways to facilitate e-commerce, customer service, input procurement, and employee connectivity, and they continue to reach significant penetration in various business sectors. Most large businesses are hosting web services, and over 50% of small businesses are now offering web accessibility [10]. As such, web security has become critically important for most organizations, and the prevention of security compromises enabled by web vulnerabilities is gaining increasingly the attention of company leadership and the broader security community. Nevertheless, web vulnerabilities are the likely causes of many recent security breaches contributing to massive disclosure of user data, leakage of business information, and other losses.

To reduce the number of web vulnerabilities, organizations can use automated web vulnerability scanners which however have been shown to only have limited coverage [16, 37]. In response, organizations more recently started to directly collaborate with or indirectly benefit from outside security researchers. These so-called *white hat* researchers spend time to analyze organizations' web systems and report vulnerabilities to self-run bug bounty programs of organizations such as Facebook, Github and PayPal, or to corresponding programs on third-party *bug bounty platforms* such as Wooyun, HackerOne, BugCrowd, Cobalt, etc.

White hats contribute in many positive ways to the discovery of web vulnerabilities. First, they can complement the limitations of automated scanners [16] by reaching deeper states of web applications, and may better understand the application logic. Second, with a mindset comparable to attackers, white hats are good at finding many exploitable vulnerabilities of high severity. Third, the large and diverse group of potential white hat contributors outnumbers internal security teams or penetration testing teams and could therefore cover a wider range of security issues.

White hats' considerable efforts are rewarded in different ways. Organizations or bug bounty platforms may provide monetary incentives based on severity and originality of the discovered issue, or publicize white hats' contributions to enhance their reputations. Previous studies and reports have shown that the cost of utilizing the white hat community may be lower compared with hiring internal security researchers [20] or using services from penetration testing companies [5].

The resulting interactions extend beyond organizational boundaries and form *web vulnerability discovery ecosystems* including businesses/organizations, white hats, and third-party vulnerability disclosure reward/bounty programs (Figure 1). These ecosystems have been growing rapidly and are becoming more prominent in the battle against malicious actors on the Internet. However, detailed studies of these web vulnerability ecosystems to understand their characteristics, trajectories, and impact are notably absent.

In this work, we conduct the first empirical study of two major web vulnerability discovery ecosystems. We base our analyses on publicly available data. The first dataset is collected from Wooyun[1], the predominant and likely the oldest web vulnerability discovery ecosystem in China. Our data contains 64,134 vulnerabilities affecting a total of 17,328 or-

CCS'15, October 12–16, 2015, Denver, Colorado, USA.
 ISBN 978-1-4503-3832-5/15/10 ...$15.00.
http://dx.doi.org/10.1145/2810103.2813704.

[1] www.wooyun.org

Platforms	Start	HQ	# Vuln.	# WHat	# Org.	Bounty Paid	Disclosure
Wooyun	**2010-07**	**China**	**64,134**	**7,744**	**17,328**	**Unknown**	**Full**
Facebook (2013) [4]	2011-08	US	687	330	1	$1.5M	No
BugCrowd [14]	2012-09	US	7,958	566	166	$0.7M	No
Loudong 360	2013-03	China	54,727	14,104	2,271	$0.7M	Partial
Cobalt	2013-07	US	8,119	2,600*	230	Unknown	Partial
HackerOne	**2013-11**	**US**	**10,997**	**1,653**	**99 (Public)**	**$3.64M**	**Partial**
Vulbox	2014-05	China	10,000	20,000*	Unknown	Unknown	Partial
Sobug	2014-05	China	3,270	8,611*	285	$0.8M (Budget)	Partial

Table 1: Statistics for representative bug bounty platforms sorted by their start time. The two platforms studied in this paper are highlighted. Numbers were obtained from the cited references, or platforms' websites directly in early August of 2015. The exact definitions of each metric for different platforms may vary. For example, some platforms count registered white hats (marked with *), while others such as HackerOne count white hats that have made at least one valid contribution.

ganizations including almost all popular Chinese web companies. We additionally collect publicly available data from HackerOne[2], a US-based start-up company which hosts bug bounty programs for hundreds of organizations, such as Yahoo, Mail.ru and Twitter, from many parts of the world. The Wooyun dataset is larger due to its coercive participation model for involving organizations, and also contains more detailed vulnerability information due to its delayed full disclosure policy. The HackerOne dataset is smaller and not all of its reports can be accessed. However, it covers a different set of organizations and also contains monetary reward information that does not exist for the Wooyun dataset. By combining these two complementary datasets, we are able to explore a wide range of topics and gain a better understanding of the structure and dynamics of such ecosystems and their impact on Internet security. We anticipate that our study will be a valuable reference for organizations who want to create or optimize their existing bounty programs.

We make the following contributions:

- Our analysis shows how many white hats have been attracted by these ecosystems and how the number of contributing white hats evolves over time. We further assess their diversity in terms of productivity and breadth of vulnerability discovery (e.g., types of vulnerabilities and affected organizations) by studying individual contributions but also contributions by groups of white hats with high/medium/low productivity. We also analyze the potential (learning) value of disclosing vulnerabilities to the white hat community.

- We then quantitatively analyze participating organizations from several dimensions, including the vulnerability trends, the coverage of different business sectors, the response and resolve behaviors, and reward structures. We evaluate the trend of reported vulnerabilities for representative organizations.

- Our study further measures the impact of different factors on vulnerability discovery. In particular, we quantify the effect of offering monetary incentives for attracting white hats and reporting discovered vulnerabilities. Based on these analyses, we discuss the benefits of disclosing vulnerability information, offer suggestions on how to improve the effectiveness of the collaboration between white hats and organizations, discuss insights for relevant policy making (e.g., the Wassenaar Arrangement), and identify important research questions for future studies.

[2]`hackerone.com`

We proceed as follows. In Section 2, we discuss related work. In Section 3, we provide background information about Wooyun and HackerOne, and discuss the collection of the datasets. We present our data analysis results in Section 4, and provide a discussion in Section 5. We offer concluding remarks in Section 6.

2. RELATED WORK

2.1 Software Vulnerability Datasets

Previous work has studied various *software* vulnerability datasets to understand vulnerability discovery, patching and exploitation. This research is relevant for the debate on whether vulnerability disclosure programs are beneficial to society [18]. That is, if the number of potential vulnerabilities is large with respect to the effort of white hats, and vulnerabilities are found in no particular order, then black hats could frequently discover and exploit vulnerabilities that are not covered by white hats' contributions; thereby questioning their effectiveness. On the one hand, Rescorla studied the ICAT dataset of 1,675 vulnerabilities and found very weak or no evidence of vulnerability depletion. He thus suggested that the vulnerability discovery efforts might not provide much social benefit [34]. On the other hand, this conclusion is challenged by Ozment and Schechter, who showed that the pool of vulnerabilities in the foundational code of OpenBSD is being depleted with strong statistical evidence [31, 32]. Ozment also found that vulnerability rediscovery is common in the OpenBSD vulnerability discovery history [31]. Therefore, they gave the opposite conclusion, i.e., vulnerability hunting by white hats is socially beneficial. More recently, Shahzad et al. [36] conducted a large-scale study of the evolution of the vulnerability life cycle using a combined dataset of NVD, OSVDB and FVDB. Their study provided three positive signs for increasing software security: (1) monthly vulnerability disclosures are decreasing since 2008, (2) exploitation difficulty of the identified vulnerabilities is increasing, and (3) software companies have become more agile in responding to discovered vulnerabilities. In another study, Frei et al. studied a security ecosystem including discovers, vulnerability markets, criminals, vendors, security information providers and the public, based on 27,000 publicly disclosed vulnera-

bilities [21]. They focus on vulnerability exploits and patching of native software, while we study the ecosystem around the discovery of web vulnerabilities, and our main focus are the behaviors and dynamics of white hats and organizations that compose such ecosystems.

2.2 Vulnerability Discoverers

Most of the existing research on software security focuses on vulnerabilities, affected software products or vulnerability discovery tools. More recently, researchers started to pay attention to the humans who make vulnerability discoveries. Edmundson et al. conducted a code review experiment for a small web application with 30 subjects [17]. One of their findings is that none of the participants was able to find all 7 Web vulnerabilities embedded in the test code, but a random sample of half of the participants could cover all vulnerabilities with a probability of about 95%, indicating that a sufficiently large group of white hats is required for finding vulnerabilities effectively. This is consistent with our analysis in Section 4.2.2 and Section 4.3.7. However, the code review process they focused on is mainly conducted inside an organization with source code available; while the vulnerability hunting focused on in this paper is conducted outside an organization. Finifter et al. provided contribution and payment statistics of participants in Google Chrome VRP and Mozilla Firefox VRP [20], and suggested that VRPs are more cost-effective compared to hiring full-time security researchers. Previous work has also reported that many discoverers primarily rely on their expertise and insights, and limited types of tools such as fuzzers and debuggers, rather than sophisticated automated vulnerability discovery tools [12, 19]. Zhao et al. conducted an initial exploratory study of white hats on Wooyun [38] and uncovered the diversity of white hat behaviors on productivity, vulnerability type specialization, and discovery transitions.

2.3 Vulnerability Markets

Böhme offers a terminology for organizational principles of vulnerability markets by comparing bug challenges, vulnerability brokers, exploit derivatives and cyber-insurance [13]. Algarni and Malaiya analyzed data of several existing vulnerability markets and showed that the black market offers much higher price for zero-day vulnerabilities, and government agencies make up a significant portion of the buyers [12]. Ozment proposed a vulnerability auction mechanism that allows a software company to measure its software quality based on the current bounty level, and to conduct vulnerability discovery at an acceptable cost [30]. This auction model can potentially be incorporated into today's vulnerability discovery ecosystems. A panel discussion at the New Security Paradigms Workshop examined ethics and implications for vulnerability markets [18]. Finally, Kannan and Telang showed that unregulated vulnerability markets almost always perform worse than regulated ones, or even no market at all [24]. They also found that it is socially beneficial to offer rewards for benign vulnerability discoverers.

3. METHODOLOGY

3.1 Analysis Overview

We organize our analysis around three components: the vulnerabilities disclosed, the white hats, and the involved businesses/organizations. Figure 1 outlines the structure of a representative web vulnerability discovery ecosystem. In the following, we describe our data collection efforts.

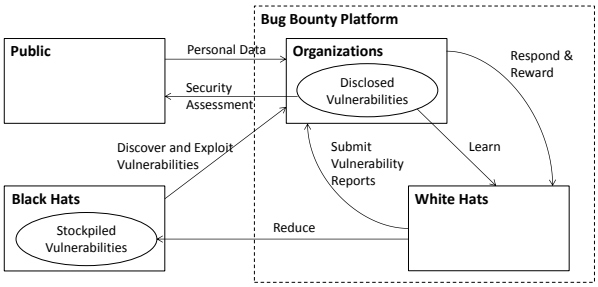


Figure 1: Structure of a web vulnerability discovery ecosystem.

3.2 Data Collection

We have collected publicly available data from Wooyun and HackerOne. The processed data and related Python scripts can be shared upon request in order to reproduce and extend our research.

3.2.1 Wooyun

Wooyun is the predominant web vulnerability disclosure program in China launched in May 2010. It has attracted 7,744 white hats who contributed 64,134 vulnerability reports related to 17,328 organizations. In most cases, Wooyun does not offer monetary rewards.

We choose Wooyun as one of the data sources for our study for several reasons. First, Wooyun insists on a delayed full disclosure policy, which states that the vulnerability will be disclosed 45 days after the submission of the report, irrespective of whether the organization has addressed the issue or not. To the best of our knowledge, it is the only platform that has such a disclosure policy. We will focus on this aspect in Section 5.1. Second, Wooyun covers the longest period of time and the largest number of contributions compared with other platforms (Table 1). It also includes a large number of organizations from several different sectors, as we will discuss in Section 4.3.3. This is because Wooyun has a very relaxed submission rule compared with other US-based platforms: white hats can submit a vulnerability report to Wooyun for almost any organization, and Wooyun will publish it as long as the report is considered valid.

We crawled the vulnerability reports on Wooyun published from May 2010 to early August 2015. For each vulnerability report, we collected the following data fields: (1) white hat's registration name, (2) target organization, (3) vulnerability type, (4) severity and (5) submission time. We further explain key data types below.

Vulnerability type: Each vulnerability report on Wooyun has a vulnerability type from a predefined list. However, we also observe that for some reports, the vulnerability types used are not in the list, possibly due to mistakes. We manually corrected these instances. We also translated the types from Chinese into English and list them in Figure 5.

Severity: The severity level of a vulnerability reflects its impact on the target organization. There are three levels: high, medium and low. We mainly use the severity level assigned by the affected organization or by the Wooyun plat-

form. If this information is missing (e.g., when the organization does not respond to the report), we will use the severity level provided by the white hat reporter.

We have also collected the following data:

Organization website's URL and Alexa rank: To examine whether a website's popularity is related to vulnerability discovery, we collected the website's rank from the Alexa Top Sites service. Since Wooyun does not provide the URL for all organizations, we wrote a script that queries the organization's name on Google and takes the first result as the URL. We then retrieved the Alexa rank of all websites from the Alexa Top Sites service. Since most websites on Wooyun are Chinese, we use the Chinese Alexa rank, rather than the global rank.

Organization sector: We also categorized organizations into different sectors. The definition of sectors are based on previous studies [15, 6]. The categorization is initially based on patterns in the organization's name. For example, universities have names like "XX university" or "university of XX". After this step, we further manually categorized the remaining organizations that have received more than 40 vulnerabilities into different sectors.

Our dataset cannot contain all vulnerabilities discovered by white hats for organizations. First, due to the large volume of vulnerability reports received, Wooyun may ignore vulnerabilities that are considered irrelevant or of very low importance, such as many reflected XSS vulnerabilities [2]. The impact of this initial expert selection is ambiguous, but we expect that our analysis may benefit from a heightened focus on valuable contributions. Second, white hats are starting to use alternative platforms such as Vulbox which do not have a public disclosure policy. As Wooyun remains the dominant platform for Chinese website vulnerabilities, we anticipate that the latter effect is relatively small.

3.2.2 HackerOne

HackerOne is a US-based bug bounty platform started in November 2013. As of early August 2015, it facilitates 99 public bug bounty programs for global companies such as Yahoo, Mail.ru and Twitter. Unlike Wooyun, white hats on HackerOne can only submit reports for these organizations. HackerOne also hosts invitation-only programs. To be eligible white hats must reach a reputation score threshold. Similar programs, such as BugCrowd also separate bounty programs into public and invitation-only [14]. Unfortunately, invitation-only programs cannot be accessed publicly, so our dataset only includes public programs.

Our HackerOne dataset includes contributions from 1,653 white hats. An organization can either reward white hats with reputation scores or monetarily compensate them. Unlike Wooyun, HackerOne does not have a delayed public disclosure policy. A vulnerability report can only be disclosed if both the white hat and the organization commit to its publication. As a result, only a small fraction (732 of 10,997) of all reports are publicly disclosed. For other reports, we only know limited metadata, including submission times, white hat identifiers, and the names of the affected organizations for each vulnerability. We are able to collect the metadata of 6,876 reports from public bounty programs in total. They constitute 62.5% of all resolved reports. We assume the remainder to be reports for invitation-only programs. In addition, HackerOne hosts bounty programs for several open source software projects, such as Perl, Python, OpenSSL. We exclude 69 reports for these bounty programs since they are not related to web vulnerabilities. Our data includes 3,886 reports with bounties paid during the study period. However, some organizations choose not to disclose the bounty amount; i.e., only 1,638 reports have exact monetary payment information. We calculate the average amount of monetary reward paid by an organization, and refer to this value as the *expected reward*.

4. RESULTS

4.1 Vulnerability Disclosure Trends

We first provide an overview of the disclosed vulnerabilities. Since the HackerOne dataset does not include data about the vulnerability type and severity, we will mainly focus on the Wooyun dataset.

4.1.1 Number of Vulnerabilities

The number of vulnerabilities accepted by the bug bounty platforms provides an initial overview of the productivity of the web vulnerability discovery ecosystems, and also reflects the time trend of web security. Table 1 shows that each of the major bug bounty platforms has published a large number of vulnerability reports. Figure 2 further displays the number of vulnerabilities accepted by Wooyun and HackerOne every month. For Wooyun, the number of vulnerabilities accepted per month continues to grow rapidly in the 5-year span. After an initial growth, the number of vulnerabilities for HackerOne's public bounty programs is relatively stable at around 400 per month. We suspect that an inclusion of data for invitation-only programs would also result in an upward trend for the HackerOne trajectory.

4.1.2 Severity Levels

We break down the overall vulnerability trend on Wooyun by severity in Figure 3. While the percentage of low severity vulnerabilities is decreasing, the percentage of published high severity reports is increasing over time. One known reason is the intentional omission of certain low severity reports, as we have discussed in Section 3.2.1. It is also possible that white hats are becoming more skilled in finding severe vulnerabilities over time. Another hypothesis is that low severity vulnerabilities are easier to discover and thus are usually reported well before more severe problems. Further investigation of these possible causes would be an interesting research question. Overall, the displayed trend indicates that organizations inside this ecosystem are still at risk, and more efforts from both the white hat community and the involved organizations are required.

4.1.3 Vulnerability Types

We next examine vulnerability reports on Wooyun according to their types. Figure 4 shows the trend for the top 3 most common vulnerability types. While the percentage of XSS reports is decreasing (possibly due to filtering as mentioned previously), we observe a small relative increase of SQL injection reports. The high amount of XSS is expected for web applications; other platforms, such as BugCrowd, have also reported that XSS is the most common vulnerability type (17.9%) [14]. In contrast, the high amount of SQL injection vulnerabilities on Wooyun is particularly surprising, since SQL injection vulnerabilities are not common on other platforms such as BugCrowd (only 1.3%) [14]. A

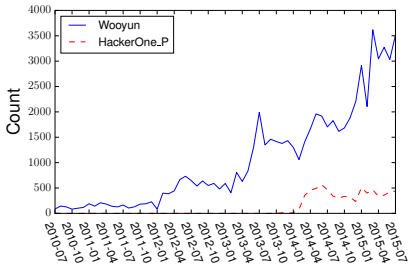


Figure 2: Number of vulnerabilities reported per month on Wooyun and HackerOne (public data).

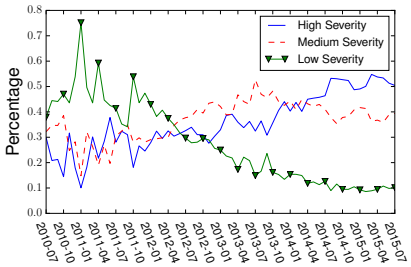


Figure 3: Trend of vulnerabilities with different severity on Wooyun.

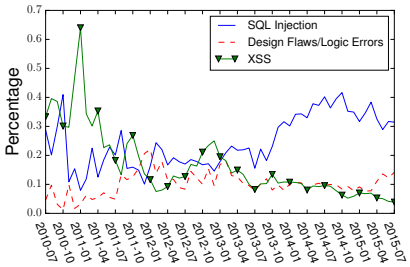


Figure 4: Trend of top 3 vulnerability types on Wooyun.

recent study also reveals that many Chinese websites are generally less secure [15]. However, the observed differences could also be caused by the particular organization participation model of Wooyun, which is able to cover much more poorly secured websites. We will discuss more on this in Section 5.4.

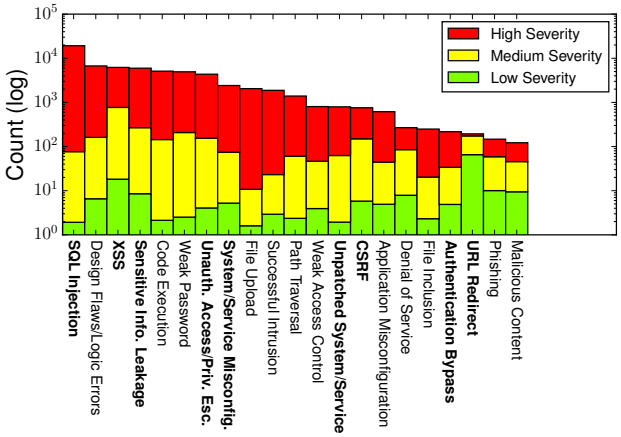


Figure 5: Number of reports for each vulnerability type on Wooyun (log scale). The compact visualization uses three colors to represent the percentage of three severity levels. Note that percentages are not affected by the log scale. Types in bold font also appear in OWASP's 2013 top 10 [1].

Figure 5 further shows the number of published reports, and the breakdown in severity categories for all vulnerability types on Wooyun. The distribution across vulnerability types is comparable to other sources [14, 1]. We also observe that some types have a larger proportion of high severity vulnerabilities; for example, SQL injection attacks and malicious file uploads may frequently open up a direct pathway to sensitive data.

In summary, data from bug bounty platforms can be used to meaningfully aggregate valuable security information. Disclosing such information, even at the aggregate level, can help the defense side to update its strategies and to allocate resources against different types of threats.

4.2 The White Hat Community

In this section, we first look at the size and growth of the white hat communities on Wooyun and HackerOne. Then, we discuss significant differences regarding productivity and accuracy among white hats using the two datasets. Next, we investigate different skills and strategies of white hats. Finally, we analyze how disclosure of reports can have positive effects on the white hat community.

4.2.1 *Size and Growth*

The outcome of a web vulnerability discovery ecosystem is closely related to the size of the white hat community, who is the "supplier" of vulnerability reports. Table 1 shows that these ecosystems have accumulated large white hat communities with tens of thousands of contributors, who may come from all over the world [14, 4]. Later, we will analyze how the size and the diversity within the white hat community correlate with vulnerability discovery outcomes.

We first examine how the size of the white hat community changes over time, using two metrics: the number of white hats who reported at least one vulnerability in each month (*active white hats*), and the number of white hats who submitted their first vulnerability in each month (*new white hats*). The difference between the number of active white hats and the number of new white hats is the number of repeat contributors. We report these two metrics for Wooyun and HackerOne in Figure 6. For Wooyun, the number of active white hats per month gradually grows to 700 per month. The number of new white hats per month is about 200 in the past 2 years, which means that there is a relatively constant flow of newcomers joining the ecosystem. The trend for the public programs of HackerOne is similar. In summary, both platforms attract a relatively constant number of white hats who contribute in a given month, while the overall size of the white hat community keeps increasing.

4.2.2 *Productivity and Accuracy*

While the size of the community matters, we also care about the individual productivity of a white hat, i.e., the number of vulnerabilities found by each white hat. In Figure 7, we plot the distribution of vulnerabilities found by individual white hats on both Wooyun and HackerOne. We observe that the distributions on both platforms are very skewed. Of 7,744 white hats on Wooyun, the top 1 has found 521 vulnerabilities, the top 100 have published more than 147 reports per person on average, but 3725 of the white hats have contributed only once. Similar observations can be made for white hats on HackerOne. Such long-tail pattern has also been found in other domains, such as scientific productivity [26].

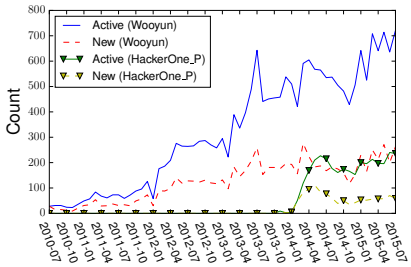


Figure 6: Number of new white hats and active white hats per month on Wooyun and HackerOne.

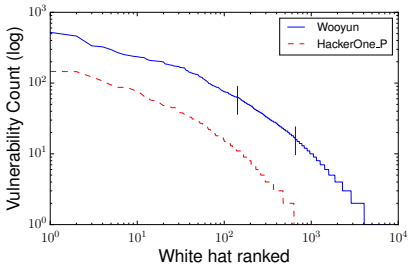


Figure 7: Contribution count of white hats on Wooyun and HackerOne (log-log). Vertical bars: thresholds for different productivity groups on Wooyun.

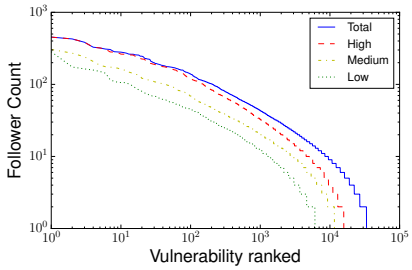


Figure 8: Distribution of follower count for vulnerabilities with different severity (log-log).

Another important aspect associated with productivity is accuracy. Many existing public bounty programs have complained about the low signal-to-noise ratio and the effort required to deal with a large amount of invalid reports, which generally include duplications, non-security issues, out-of-scope, false positives, or even spam [14, 9, 4, 8]. The signal-to-noise ratio is roughly 20% for platforms such as HackerOne and BugCrowd, and even lower for individually hosted bounty programs by Facebook and Github [14, 8]. In addition, HackerOne has reported that in general more productive researchers have a higher signal-to-noise ratio [8]. Based on [8], we estimate that the top 1% researchers on HackerOne have an average ratio of 0.54, while the bottom 50% only have an average ratio of 0.03, indicating that approximately among 100 reports submitted by them, only 3 are expected to be valid vulnerability reports. Bug bounty platforms have introduced various data-driven approaches, including reputation systems and rate limiting, to improve the signal-to-noise ratio [8]. This partly explains the higher signal-to-noise ratio of bounty platforms over individually hosted bounty programs. However, the low signal-to-noise ratio remains a key challenge for effective vulnerability discovery and requires more research effort.

The long-tailed distribution of contribution levels as well as concerns about accuracy lead to an increased focus on the top contributors in today's bug bounty programs, since they are on average much more productive, and more accurate. As a result, existing bounty platforms such as HackerOne and BugCrowd have created private bounty programs that only invite a small number of top contributors [14, 9, 8]. In some cases, the top contributors were directly hired by organizations or bounty platforms [4, 7].

Less attention is given to white hats with lower productivity. However, taken as a group, they contribute a sizable number of accepted reports. As such, the question arises how to evaluate their contributions. To do an initial comparative assessment, we split the white hat community on Wooyun into three groups of different levels of productivity. The two thresholds, displayed in Figure 7, are chosen so that the three groups have approximately the same number of reports, thus allowing us to compare other dimensions of their contributions.

We report the results in Table 2. Unsurprisingly, the average number of accepted reports differs substantially across these groups. In contrast, an interesting observation is that the less productive groups have contributed reports for a considerably larger number of organizations. There could be multiple reasons to explain this difference. First, the less productive groups have many more white hats, leading to more "manpower" and more diverse interests covering a wider range of websites. Meanwhile, white hats in the highly productive group have more limited attention or may benefit from an increased focus on a specific set of websites. Second, some websites may have been particularly popular targets for white hats, and easy-to-be-found vulnerabilities are already removed. For many low productive white hats who may also have limited expertise, spending effort on such websites might not be cost-effective. Thus, they shift their attention to other websites, which are more likely to yield discoveries.

	Productivity Groups		
Variable	**High**	**Medium**	**Low**
# white hats	142	658	6,972
Total # vuln.	17,611	17,586	17,595
Average # vuln.	124	27	2.5
# contributed org.	4,727	5,686	7,247
Alexa 1-200 (%)	32.5	34.4	33.1
Alexa 201-2000 (%)	32.4	33.6	34.0
Alexa > 2000 (%)	33.7	32.9	33.3
Severity High (%)	38.4	33.5	28.1
Severity Medium (%)	31.3	32.5	36.1
Severity Low (%)	25.1	34.5	40.4

Table 2: Comparison across three white hat groups of different productivity levels on Wooyun.

The broader coverage of websites by less productive white hats has a positive impact on the security of the Internet, since even less popular sites still receive a considerable amount of visitors every day. In addition, the security of organizations is rather connected in many ways [22, 33]. For example, a user could use the same username and password across multiple sites, and the compromise of one of them will jeopardize others. Therefore, by complementing the limited attention of top white hats, the less productive white hat groups make different but important contributions.

We further break down the contributions of each group by target websites' popularity and by vulnerability severity. Rows 5 - 7 of Table 2 show that for the different popularity categories the contributions (in %) across the three productivity groups are remarkably consistent. In particular, the

least productive group also reports a significant percentage of discoveries for popular websites. Row 8 shows that more productive white hats have a larger percentage of contributions with high severity vulnerabilities, but 28.1% of high severity vulnerabilities were still discovered by the least productive white hats.

In summary, the results support the existence of a substantial expertise and productivity gap on an individual level, but from a collective perspective the difference is smaller than perhaps expected. How to better utilize the potential of these different groups of white hats is an interesting challenge. In particular, it would be useful to think about how to boost the productivity of less productive white hats through better incentives, training, and other measures.

4.2.3 Skills and Strategies

Next to productivity, we measure two additional metrics: the number of different organizations an individual white hat investigated, and the number of different vulnerability types an individual white hat reported. These two metrics partly reflect the skills, experiences and strategies of white hats. Figure 9 shows the distribution of these two metrics for white hats on Wooyun with more than 5 discoveries. The average number of organizations investigated by a white hat of this group is 18, while the average number of vulnerability types found is 7. The most productive individuals (i.e., red triangles in the figure) generally surpass others in both metrics which partially explains the productivity difference. First, top white hats' broad knowledge of different types of vulnerabilities may enable them to discover more vulnerabilities. Second, they may find more vulnerabilities because their strategy is to investigate a larger number of websites. Furthermore, we hypothesize that there is a trade-off between exploration vs. exploitation: to find more vulnerabilities, a white hat must develop a good balance between spending effort at one particular website and exploring opportunities on other sites. However, different successful strategies coexist. For example, our dataset includes several white hats in the bottom left corner of Figure 9 that is much more focused on exploitation. Similarly, a white hat named 'meals' ranked 4th on HackerOne only focuses on Yahoo's bounty platform, and has to-date found 155 vulnerabilities.

Investigating the optimal degree of strategy diversification during web vulnerability hunting is an interesting area for future work.

4.2.4 Disclosure and Learning

A primary consideration of previous research was to understand how vulnerability disclosure pushes software vendors to fix flaws in their products [35, 36]. However, when considering the whole ecosystem, we question whether vulnerability disclosures also have positive effects on the white hat community itself. One possible effect is to enable white hats to learn valuable technical insights and skills from others' findings. Another effect is to obtain valuable strategic information for their own vulnerability discovery activities, such as which organizations to investigate. Both effects likely improve white hats' productivity and accuracy. In addition, the software engineering community and peer organizations can also learn valuable lessons from vulnerability reports to avoid making similar mistakes in the future. While the latter factor may be of high practical relevance,

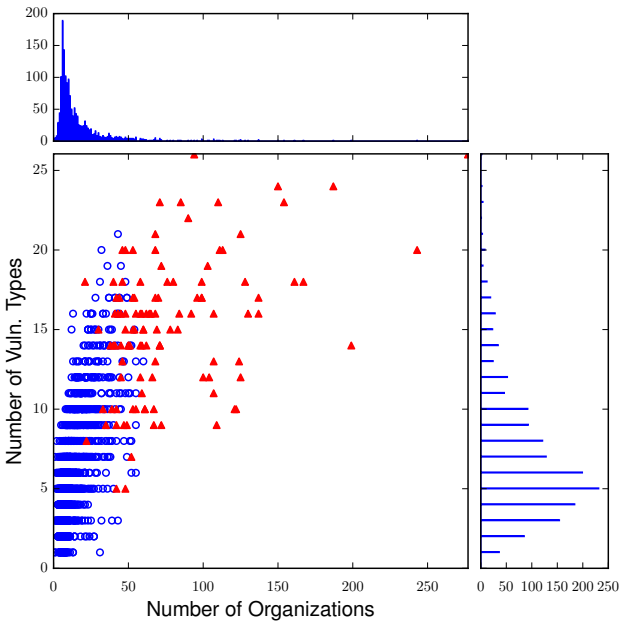


Figure 9: Scatter plot of white hats' vulnerability type count and targeted organization count on Wooyun. Each dot represents a white hat who has found more than 5 vulnerabilities in total. The red triangle dots are white hats of the high productivity group defined in Section 4.2.2.

we are unaware of related research. In this paper, we investigate the first effect using data from Wooyun.

The Wooyun platform allows white hats to mark and follow a particular report. Therefore, we can use the number of followers of a vulnerability report as an approximate indicator of its learning value to white hats. In Figure 8, we plot the distribution of this follower count for all vulnerabilities on Wooyun, and also break down the data by different severity levels. We observe that the distribution is very skewed. There are 9,489 reports that have at least 10 followers, indicating that white hats have been actively learning from a broad portion of reports. On average, high severity vulnerabilities have more followers, which is not surprising, as more severe vulnerabilities tend to have a more significant security impact, and higher discovery and exploit complexity. What might be counter-intuitive is that some low severity vulnerabilities still receive more than 100 followers.

To examine why some vulnerabilities have received much more attention than others, and why some low severity vulnerabilities are followed by many, we selected the 30 most followed vulnerabilities from each severity level. We then manually examined these 90 vulnerabilities. We find that these vulnerabilities mostly belong to one or more of the following categories: (1) Vulnerabilities with significant impact (e.g., with a potential for massive user data leakage, or an XSS inside the site statistics javascript code from a major search engine company); (2) Vulnerabilities that are associated with novel discovery or exploitation techniques; (3) Vulnerabilities of widely used web applications, such as CMS; (4) Vulnerabilities that are explicitly organized as tutorials. We found 21 such tutorial-style reports belonging to a series about XSS, which are all of low severity, yet they

still receive a lot of attention because of the emphasis on learning. We also examined a subset of disclosed reports from HackerOne and have discovered that some organizations make disclosures[3] to teach the writing of concise reports.

In summary, our analysis provides evidence of how white hats are learning from vulnerability reports; a typically overlooked benefit of vulnerability disclosure to the white hat community. We will discuss additional facets of disclosure in Section 5.1.

4.3 Organizations

We now shift our focus to the organizations who have participated in vulnerability discovery ecosystems. These organizations harvest vulnerability reports from the white hat community, fix security flaws, and thereby ultimately improve the security of the whole Internet (e.g., by reducing the impact of security interdependencies [22, 33]). However, collecting data about them is non-trivial because many organizations, such as banks, are still reluctant to collaborate with white hats due to various concerns [3]. In addition, for many organizations who joined platforms such as HackerOne, data about discovered vulnerabilities, monetary rewards and other important factors is often not publicly disclosed.

Wooyun provides a valuable opportunity to study the impact of such ecosystems on organizations; and not only because of the existence of the delayed public full disclosure policy. More importantly, an organization is rather coerced to join this ecosystem once a white hat publishes a vulnerability on Wooyun affecting the organization. This *coercive model* is different from most other platforms which only host bounty programs for organizations that agree to participate (i.e., *voluntary model*). Due to the diversity of the large white hat community, Wooyun covers a broad range of organizations from many sectors, as we will show in Section 4.3.3. As a result, observations made from this dataset do not only help us understand the web vulnerability discovery ecosystem in China, and the general security status of the Chinese web, but also help us to envision the impact of the bug bounty model for organizations in other parts of the world.

4.3.1 Size and Growth

Table 1 lists the number of organizations participating in representative vulnerability discovery ecosystems. We observe that Wooyun affects a larger number of organizations compared with US-based platforms, who typically have tens or hundreds of participating organizations. The difference is partly due to the coercive versus voluntary ways of involving organizations. Therefore, the Wooyun ecosystem roughly represents an upper bound of coverage (growth) for other ecosystems. We also investigate the trajectory of the growth of the number of organizations covered on Wooyun. Figure 10 shows that in every month, there are about 300 organizations benefiting from white hats' efforts. Around 150 of them are new organizations, which implies that the white hat community is continuously broadening its horizon. It would be interesting to understand whether this effect relies on the fact that new businesses are founded (or new websites become public), or that white hats are moving to already established but previously unresearched websites.

[3]For example: `https://hackerone.com/reports/32825`.

4.3.2 Vulnerability Distribution

For both Wooyun and HackerOne, Figure 11 shows that only few organizations receive a high number of vulnerability reports, while most organizations receive very few vulnerability reports. We hypothesize that the number of vulnerabilities received by organizations is related to multiple factors, such as the complexity of the web system, the existence of monetary incentives, the popularity of the website, etc. We will further investigate the relation between these factors and the number of published vulnerability reports in Section 4.3.7.

4.3.3 Impact on Different Sectors

To investigate the diversity within participating organizations, we have manually tagged organizations on HackerOne based on their business types. We find that *all* participating companies are IT-focused and cater to different business/consumer needs which are shown in Table 3.

social network (13), security (9), content sharing (9)
payment(8), communication (8), bitcoin (6),
cloud (5), customer management (5),
site builder (5), finance (4), ecommerce (4)

Table 3: Frequency of IT-business types within the group of publicly available bounty programs on HackerOne. Only tags with frequency greater than 3 are shown.

Due to its coercive model for involving organizations, the Wooyun dataset includes a larger and more diverse set of organizations (see Figure 12). Further, it shows that white hats do not exclusively focus on certain business sectors.

For non-IT organizations, two sectors with many vulnerability reports are government and finance. We consider this finding surprising since these sectors have robust incentives for security investments. While the finance sector, and possibly the government sector as well, are often not willing to collaborate with non-commercial white hats [3], we infer from the Wooyun data that they can disproportionally benefit from the involvement of the white hat community. Participating in disclosure programs may also reduce the likelihood that vulnerabilities flow into the black market [21].

Portal sites, telecommunication and e-commerce organizations have the highest number of vulnerability reports in the IT-sector. A possible explanation is that web services and systems from these domains are large and complex which increases the amount of latent vulnerabilities. Further, these companies serve substantial user populations which increases their desirability for vulnerability researchers.

4.3.4 Response and Resolution

After the initial submission of a vulnerability report, the typical follow-up process on most bounty platforms contains the following steps: triage/confirm, resolve, and disclose. During this process, the white hat and the security/development team of the organization may collaborate together to address the identified problem. A delayed response likely increases the risk of a security breach, since it increases the time frame for rediscovery of the vulnerability, and stealthy exploitation of stockpiled vulnerabilities by malicious agents. Given its full disclosure policy, a delayed response to a submission on Wooyun may be even more serious because details will be disclosed publicly after 45 days.

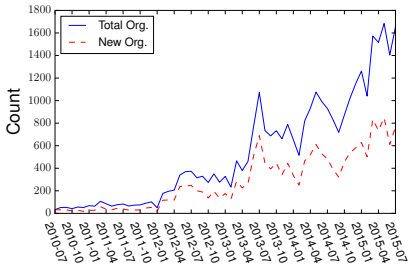


Figure 10: Count for new and total number of organizations with vulnerability reports (per month) on Wooyun.

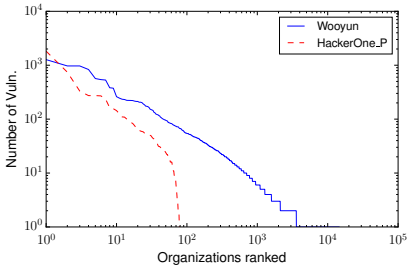


Figure 11: Number of vulnerabilities by organizations on Wooyun and HackerOne.

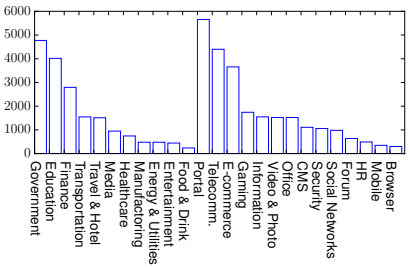


Figure 12: Number of vulnerability reports for non-IT businesses (left), and IT-sector businesses (right) on Wooyun.

Our data allows us to examine how organizations respond and resolve vulnerability reports in the studied ecosystems. HackerOne maintains a detailed handling history for each vulnerability report. Unfortunately, only a small portion of all resolved reports (732 of 10,997) are publicly disclosed. For these disclosed reports, we determined the time distribution for three types of response activities (see Figure 13). The median time for the first response (e.g., a confirmation of receiving the report) is 0.18 days, and the median time for triage is 0.88 days. The median resolve time is 6.49 days, and 75% of the disclosed reports are resolved in 25 days. However, one should be cautious when generalizing from these observations since the data is possibly biased. Particularly, the analysis likely underestimates the time required for triaging and resolving vulnerabilities, since the organizations that are willing to disclose vulnerabilities may be more efficient in handling reports and may have more experience in running bounty programs.

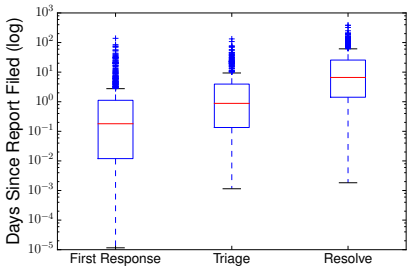


Figure 13: Boxplots for the time of three types of response activities based on publicly disclosed reports on HackerOne.

Wooyun shows four types of responses by organizations: confirmed by organization (CO), confirmed and handled by a third party such as CNCERT (CT), ignored by the organization (IG), and no response (NO). Since all reports are classified in this way, the Wooyun response data is considerably larger, but provides less details. For example, it is difficult to discern whether the organization eventually fixed the vulnerability (or not), but the first two types of response can serve as an indication that the organizations recognizes the problem. The third type of response suggests that the organization considers the vulnerability report invalid. The fourth type means that the organization did not respond to the report at all. We use the count of the fourth type as a rough estimate for the number of cases when an organization fails to address a vulnerability report, and consider the other three types of responses as situations when the vulnerability is likely being handled.

	CO	CT	IG	NO
Overall (%)	40	34	3	23
Organizations:				
- Alexa 1 - 200 (%)	71	13	5	12
- Alexa 201 - 2000 (%)	57	18	4	20
- Alexa > 2000 (%)	28	44	1	26

Table 4: Percentages of different types of responses by organizations on Wooyun.

Table 4 shows the percentages for the different types of response as a breakdown by the popularity of the websites. We observe that overall, the majority (77%) of the vulnerability reports have been handled. Popular websites address more vulnerabilities by themselves, while less popular websites rely more often on third parties. In addition, less popular websites have a higher rate of no response, possibly due to limited resources for vulnerability management.

4.3.5 *Monetary Rewards*

We also examine the role of monetary rewards offered by some organizations. We observe that in their absence, white hats still make contributions to Wooyun and HackerOne for the purpose of making the Internet safer and for reputation gains. For example, 33 of the public programs on HackerOne do not provide monetary rewards, yet they still have received 1201 valid reports from the white hat community. But as Table 1 shows, most platforms offer monetary rewards as an additional incentive for white hats to contribute their time and expertise.

We conduct a preliminary analysis based on the disclosed bounties for public programs on HackerOne. Given a total of 3886 bounties, 1638 have the amount information disclosed. The maximum bounty is $7560, paid by Twitter, and the average bounty amount is $424 which varies considerably by organizations. Yahoo pays $800 on average, followed by Dropbox ($702) and Twitter ($611). We hypothesize that the current reward level is attractive to many white hats, and we explore this topic in more detail with a regression study in Section 4.3.7.

4.3.6 *Improvements to Organizations' Web Security*

The participation in a bug bounty program should over time improve the web security of an organization in a noticeable way. In particular, it is reasonable to expect that the

number of latent vulnerabilities in an average organization's web systems (and the stockpile of web vulnerabilities held by black hats) would gradually diminish. Our data allows us to investigate whether the number of vulnerability reports per month is changing over time which is a relevant metric in this context. Moreover, it is a type of analysis that can be conducted by external evaluators if the bug bounty program is public, and provides stakeholders an indication of the web security of an organization. For example, the Cobalt bounty platform offers security seals for organizations that use their services, which is expected to improve the public perception of the organization's security [37]. Other services (e.g., cyber-insurance companies), can also benefit from such security assessments (e.g., for the determination of insurance premiums) [23, 25].

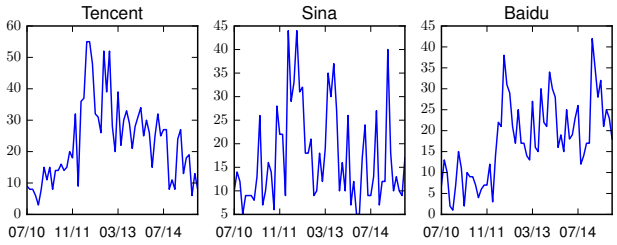


Figure 14: Trend of vulnerability report count for three organizations on Wooyun.

To initially explore this question, we show the vulnerability report trends for three large organizations on Wooyun in Figure 14. While one notices a slight decreasing trend for Tencent, it is hard to observe a clear tendency for the other two organizations. More importantly, Wooyun may not exclusively host these organizations' bounty programs which could influence the analysis.

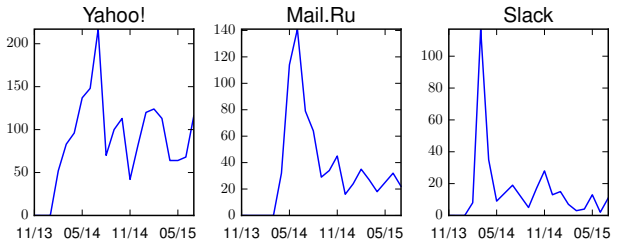


Figure 15: Trend of vulnerability report count for three organizations on HackerOne.

In contrast, HackerOne is tasked to exclusively host bounty programs for participating organizations which ensures a more reliable analysis. We show the vulnerability trends for the three organizations with the most vulnerabilities on HackerOne (Figure 15). Interestingly, these organizations have received a large volume of vulnerability reports right after the launch of their bounty programs. We propose three possible explanations. First, the monetary compensation offered by HackerOne provides stronger incentives for white hats to compete for vulnerability discoveries in the early stage of a bounty program since the bounty program only rewards the first discoverer. Second, the target range for white hats on HackerOne is much more limited compared to Wooyun, thus concentrating white hats' focus. Third, some white hats might have stockpiled vulnerabilities to offload them for reward in anticipation of the opening of new reward programs. After these initial spikes, the number of vulnerability reports on HackerOne drops significantly, possibly because the difficulty of finding new vulnerabilities is increasing. However, even though we observe decreasing trends, these organizations still receive a positive number of vulnerability reports every month. These additional discoveries may either be related to further latent vulnerabilities in existing code or stem from new code. Therefore, we suggest that organizations continuously collaborate with white hats.

To further examine the vulnerability trends for organizations, we apply the Laplace test [32] to the vulnerability history of organizations who have received at least 50 reports and have a bounty program for more than 4 months. We also excluded data before 2012-02 and 2014-02 (the initial growth periods), for Wooyun data and HackerOne data, respectively. This test indicates whether there is an increasing trend, a decreasing trend, or no trend for the number of reported vulnerabilities for a given organization (Table 5).

Platform	Decrease	Increase	No Trend
Wooyun	11	81	17
HackerOne	32	8	9

Table 5: Trend test results for organizations on Wooyun and HackerOne. The confidence level is 0.95.

Only 11 of the 109 organizations on Wooyun (which match the criteria) fit a decreasing trend, while most selected organizations have an increasing trend for the number of vulnerability reports. The data omission bias discussed previously could be one reason of the result. A sufficiently large pool of latent vulnerabilities in combination with increasing activity on Wooyun could serve as an alternative explanation. For organizations on HackerOne, 32 of 49 have a decreasing trend indicating a positive effect of the vulnerability discovery ecosystem.

The trend test, however, cannot completely assess the web security status of an organization for several reasons which we have partly discussed above. Further, as a possible part of their vulnerability discovery strategy (see Section 4.2.3), white hats might switch to new organizations or newly deployed web systems which are expected to have more low hanging fruits. In general, we suggest that a reliable assessment requires careful modeling and statistical analysis of the whole ecosystem which is an important area for future work.

4.3.7 *Attracting Vulnerability Reports*

How can an organization harvest more vulnerability reports from the white hat community to improve its web security? To address this question, we first study the correlation between the number of vulnerability reports per organization and the number of contributing white hats.

Figure 16 plots the number of white hats that have made at least one discovery, and the number of vulnerabilities, for each organizations (with at least 20 vulnerability reports) on Wooyun and HackerOne. We observe very strong positive linear (Pearson) correlations for these measures (as shown in the figures). Therefore, the following strategies are likely

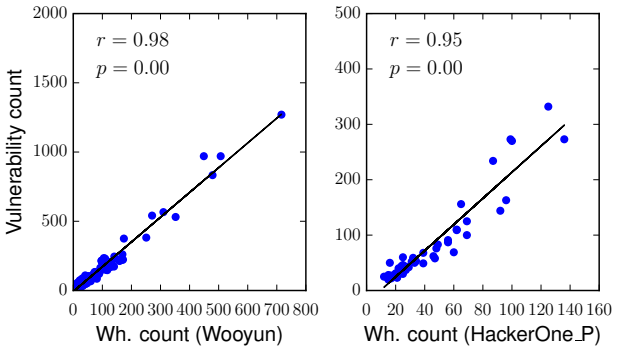


Figure 16: Scatter plots of organizations' white hat count and vulnerability count for Wooyun and HackerOne public programs (excluded Yahoo and Mail.ru as outliers).

VARIABLES	(1) # Vuln.	(2) # Vuln.	(3) # Vuln.
Expected Reward (R_i)	0.04***	0.03***	0.03***
	(0.01)	(0.01)	(0.01)
Alexa [log] (A_i)		-2.52*	-2.70**
		(1.20)	(1.21)
Platform Manpower (M_i)			10.54
			(10.14)
Constant	3.21*	16.12**	-133.05
	(1.88)	(6.39)	(143.66)
R-squared	0.35	0.39	0.40

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Table 6: Results of regression analysis. There are 60 observations (HackerOne).

beneficial: (1) While paying special attention to top contributors is a useful strategy, it is also important to increase the total number of contributors. A possible reason to explain the observed effect is that vulnerability discovery requires diversity, i.e., investigators with different expertise using different tools may find different vulnerabilities; (2) It is important to incentivize new participation, for example, by offering an extra bonus (e.g., badge or money) for the first valid submission of a white hat to a platform or specific program.

Other factors such as the popularity of the target, the expected bounty amount, and the number of alternative choices are all related to a bounty program's attractiveness to white hats. To better understand these factors, we conduct a linear regression by taking the number of vulnerability reports as the dependent variable and other factors as independent variables, as the following equation shows:

$$V_i = \beta_0 + \beta_1 R_i + \beta_2 A_i + \beta_3 M_i + \epsilon_i$$

where for each organization, V_i is the average number of vulnerabilities per month, R_i is the expected reward, A_i is the log Alexa rank of i's website, and M_i is the average platform manpower during the lifetime of organization i's bounty program. M_i is defined as the time-weighted number of white hats divided by the time-weighted number of peer organizations during the lifetime of i's bounty program:

$$M_i = \frac{NW_1 T_i + \sum_{k=2}^{T_i}(NW_k - NW_{k-1})(T_i - k + 1)}{NO_1 T_i + \sum_{k=2}^{T_i}(NO_k - NO_{k-1})(T_i - k + 1)}$$

Here, T_i is the number of months for i'bounty program. NW_k and NO_k are the accumulated number of white hats and the number of peer organizations on the whole platform at the kth month for organization i, respectively.

Table 6 shows three variations of the regression model. In all three models, we find a highly significant positive correlation between the expected reward offered and the number of vulnerabilities received by that organization per month. Roughly speaking, a $100 increase in the expected vulnerability reward is associated with an additional 3 vulnerabilities reported per month. We also find a significant negative correlation between the Alexa rank and the number of vulnerabilities in models (2) and (3) suggesting that rank determines the attractiveness of a website to white hats. However, it is also possible that less popular websites are in general less complex in design and implementation, and thus contain less vulnerabilities. For model (3), we expect that with higher average platform manpower, an organization will receive more attention from white hats and thus will have more vulnerability reports. However, the analysis does not yield a conclusive answer, possibly due to the omission of invitation-only programs and limited sample size.

The quantified model can be used by organizations when determining their bug bounty policies and attracting an effective white hat following. In particular, offering higher rewards and running the program for a longer time contributes to a higher number of reports. The model also contributes to the security assessment question in Section 4.3.6. Nevertheless, our regression model is only a first step towards modeling the dynamics of the web vulnerability discovery ecosystem. It could be extended with more independent variables, such as the business type of organizations (see Section 4.3.3), or the expected rewards from peer organizations in the ecosystem.

5. DISCUSSION

5.1 Importance of Disclosure

Based on our analysis, we believe that disclosing important information about vulnerability discovery (such as the resolve time for each vulnerability, bounty amounts, and even the detailed reports) is important for the success of a web vulnerability discovery ecosystem. For the white hat community, disclosing more vulnerability information not only enables them to learn and improve, but also potentially allows to make better decisions on target selection, as we have discussed in Section 4.2.4. The transparency associated with disclosure could also reduce conflicts between organizations and white hats on issues like the validity of a report or the reasonableness of a bounty amount. For organizations, disclosing more information enables the public (e.g., Internet users, or cyber-insurance providers) to better assess the security of an organization (Section 4.3.6). Disclosure is also vital for the research community to tackle some of the challenging issues and future research questions we have discussed. In addition, a platform such as Wooyun

with a delayed full disclosure policy also pushes organizations to fix their reports sooner.

However, there are also potentially less desirable consequences of disclosing vulnerabilities about organizations' web systems, such as the leakage of critical information that can be utilized by black hats. An ideal disclosure policy has to balance the potential benefits and disadvantages to the ecosystem or a specific organization. Several disclosure programs are moving towards this direction. For example, some programs on HackerOne disclose only a subset of their vulnerabilities to the public. The Github bounty program discloses data about every vulnerability discovered by white hats, yet intentionally redacts certain details. Further analyzing the benefits and risks of disclosing vulnerability information, and designing improved disclosure policies is important future work.

5.2 Potential Incentive Structure Evolution

Our study shows that monetary incentives increase the number of vulnerability reports (Section 4.3.7). We anticipate that more organizations will start paying bounties, as more organizations are joining vulnerability disclosure ecosystems and are competing for the limited attention of white hats. The amount of an average bounty will likely rise not only for the purpose of attracting more white hats, but also for compensating the increasing cost incurred by white hats to discover vulnerabilities (e.g., to compete with black hats). In addition, high reward amounts can also be a positive signal of an organization's security practices to the public, similar to the proposal in [30].

Many organizations will continue to not offer bounties. For small organizations with limited revenues, maintaining a competitive bounty level could be challenging. It has also been suggested that an organization could start with no bounty first, and gradually increase the reward level, to alleviate the initial surge of reports (including many invalid submissions) [27], as we have shown in Figure 15. Organizations that cannot afford paying bounties can resort to other forms of incentives, such as reputation scores, hall-of-fame memberships, or even public disclosure.

5.3 Encouraging White Hat Participation

Increasing the size of the white hat community allows more organizations to be covered and more vulnerabilities to be found (see Section 4.2.2). A larger white hat community might also decrease the cost of running bounty programs for organizations, similar to the increase of supply in any economic market. Therefore, potential regulations that hinder the collaboration between white hats and organizations are likely detrimental. One such example is the proposed update of the Wassenaar Arrangement, which aims to control the export of intrusion software. The utilized overly broad definition of intrusion software could easily limit the participation of white hats [29], particularly considering the global nature of the white hat community [4, 14].

To encourage more white hats to join the ecosystem, organizations can try to offer a first time bonus (see Section 4.3.7), organize capture-the-flag activities, etc. In addition, by analyzing the behavioral patterns and dynamics of white hats (e.g., Section 4.2.3), bounty platforms can design customized services for white hats, such as target selection or recommender systems, which match white hats' skills and organizations' requirements. For this purpose, it would be helpful to further investigate vulnerability discovery by white hats (e.g., tool usage) through interview or survey studies [19].

5.4 Stimulate Participation by Organizations

Our study results provide incentives for organizations to join vulnerability discovery ecosystems and to benefit from white hats' efforts. In addition, government agencies such as the Federal Trade Commission also encourage organizations to have a process of receiving and addressing vulnerability reports [11], which can be achieved by running a bounty program.

In our work, we contrast two participation models from the organizations' perspective. The first one is the *coercive participation model*, represented by China-based platforms such as Wooyun. That is, an organization is coerced to join the ecosystem once a white hat has submitted a vulnerability for that organization. The second participation model, represented by US-based platforms including HackerOne, is voluntary, i.e., companies explicitly authorize external researchers to study the security of their web systems. Both models have their advantages and disadvantages. Our results show that the first model is capable of covering a wider range of organizations, although varying legal conditions in different countries might not allow for such an approach (see, for example, [28]). Also, this model might allow many severe vulnerabilities to be found earlier in websites that are not willing to participate bug bounty and are poorly secured. This could partly explains the high percentage of SQL injection on Wooyun in Section 1. The coercive model might be more attractive to white hats, for example, since they may feel more in control. The second model clearly grows more slowly when considering the number of participating organizations. However, voluntary participation likely encourages a better response behavior to vulnerability reports, as we have discussed in Section 4.1.3. To encourage organizations to participate in the voluntary model, future work is needed to identify and address organizations' concerns including the perceived lack of trustworthiness of the white hat population [3], misuse of automated vulnerability scanners, and time wasted due to false reports [8].

6. CONCLUSION

In this paper, we have studied emerging web vulnerability discovery ecosystems, which include white hats, organizations and bug bounty platforms, based on publicly available data from Wooyun and HackerOne. The data shows that white hat security researchers have been making significant contributions to the security of tens of thousands of organizations on the Internet.

We conducted quantitative analyses for different aspects of the web vulnerability discovery ecosystem. Based on our results, we suggest that organizations should continuously collaborate with white hats, actively seek to enlarge the contributor base, and design their recognition and reward structure based on multiple factors. We have also proposed future work directions to help to increase the impact and coverage of these ecosystems.

Acknowledgments

We thank the anonymous reviewers for their helpful comments. The authors would also like to thank Yue Zhang, Aron Laszka, Kai Chen and Zhaohui Wu for their valuable comments on earlier drafts of this paper. Peng Liu was supported in part by ARO W911NF-09-1-0525 (MURI), CNS-1422594, and ARO W911NF-13-1-0421 (MURI).

7. REFERENCES

[1] OWASP 2013 Top 10. www.owasp.org/index.php/Top_10_2013-Top_10.

[2] Updates on vulnerability handling process. www.wooyun.org/notice.php?action=view&id=28, 2013.

[3] Banks reluctant to use 'white hat' hackers to spot security flaws. NPR, 2014.

[4] Bug bounty highlights and updates. Facebook, 2014.

[5] How Bugcrowd uses crowdsourcing to uncover security flaws faster than the bad guys do (Interview). VentureBeat, 2014.

[6] Website security statistics report. White Hat Security, 2014.

[7] CSUS student hunts for computer bugs as a 'white hat'. www.sacbee.com/news/business/article5014716.html, 2015.

[8] Improving signal over 10,000 bugs. https://hackerone.com/blog, 2015.

[9] LinkedIn's private bug bounty program: Reducing vulnerabilities by leveraging expert crowds. security.linkedin.com, 2015.

[10] Small business website statistics. www.statisticbrain.com/small-business-website-statistics/, 2015.

[11] Start with security: A guide for business. FTC, 2015.

[12] A. Algarni and Y. Malaiya. Software vulnerability markets: Discoverers and buyers. *International Journal of Computer, Information Science and Engineering*, 8(3):71–81, 2014.

[13] R. Böhme. A comparison of market approaches to software vulnerability disclosure. In *Emerging Trends in Information and Communication Security*. 2006.

[14] BugCrowd. The state of bug bounty, 2015.

[15] P. Chen, N. Nikiforakis, L. Desmet, and C. Huygens. Security analysis of the Chinese web: How well is it protected? In *Workshop on Cyber Security Analytics, Intelligence and Automation*, 2014.

[16] A. Doupé, M. Cova, and G. Vigna. Why Johnny can't pentest: An analysis of black-box web vulnerability scanners. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, 2010.

[17] A. Edmundson, B. Holtkamp, E. Rivera, M. Finifter, A. Mettler, and D. Wagner. An empirical study on the effectiveness of security code review. In *Engineering Secure Software and Systems*, 2013.

[18] S. Egelman, C. Herley, and P. van Oorschot. Markets for zero-day exploits: Ethics and implications. In *New Security Paradigms Workshop*, 2013.

[19] M. Fang and M. Hafiz. Discovering buffer overflow vulnerabilities in the wild: An empirical study. In *8th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, 2014.

[20] M. Finifter, D. Akhawe, and D. Wagner. An empirical study of vulnerability rewards programs. In *USENIX Security Symposium*, 2013.

[21] S. Frei, D. Schatzmann, B. Plattner, and B. Trammell. Modeling the security ecosystem - The dynamics of (in)security. In *Economics of Information Security and Privacy*, 2009.

[22] J. Grossklags, N. Christin, and J. Chuang. Secure or insure? A game-theoretic analysis of information security games. In *17th International Conference on World Wide Web*, 2008.

[23] B. Johnson, R. Böhme, and J. Grossklags. Security games with market insurance. In *Decision and Game Theory for Security*, 2011.

[24] K. Kannan and R. Telang. Market for software vulnerabilities? Think again. *Management Science*, 51(5):726–740, 2005.

[25] A. Laszka and J. Grossklags. Should cyber-insurance providers invest in software security? In *20th European Symposium on Research in Computer Security*, 2015.

[26] A. Lotka. The frequency distribution of scientific productivity. *Journal of Washington Academy Sciences*, 16(12):317–323, 1926.

[27] R. McGeehan and L. Honeywell. Bounty launch lessons. medium.com/@magoo/bounty-launch-lessons-c7c3be3f5b, 2015.

[28] E. Messmer. Hacker group defies U.S. law, defends exposing McAfee website vulnerabilities. *Network World*, 2011.

[29] K. Moussouris. You need to speak up for internet security. Right now. Wired, 2015.

[30] A. Ozment. Bug auctions: Vulnerability markets reconsidered. In *Workshop on the Economics of Information Security*, 2004.

[31] A. Ozment. The likelihood of vulnerability rediscovery and the social utility of vulnerability hunting. In *Workshop on the Econ. of Information Security*, 2005.

[32] A. Ozment and S. Schechter. Milk or wine: Does software security improve with age? In *USENIX Security Symposium*, 2006.

[33] S. Preibusch and J. Bonneau. The password game: Negative externalities from weak password practices. In *International Conference on Decision and Game Theory for Security*, 2010.

[34] E. Rescorla. Is finding security holes a good idea? *IEEE Security & Privacy*, 3(1):14–19, 2005.

[35] G. Schryen. Is open source security a myth? *Communications of the ACM*, 54(5):130–140, 2011.

[36] M. Shahzad, M. Shafiq, and A. Liu. A large scale exploratory analysis of software vulnerability life cycles. In *International Conference on Software Engineering*, 2012.

[37] T. Van Goethem, F. Piessens, W. Joosen, and N. Nikiforakis. Clubbing seals: Exploring the ecosystem of third-party security seals. In *ACM Conference on Computer and Communications Security*, 2014.

[38] M. Zhao, J. Grossklags, and K. Chen. An exploratory study of white hat behaviors in a web vulnerability disclosure program. In *Proceedings of the 2014 ACM Workshop on Security Information Workers*, 2014.

The Internet of Things Brings Far-Reaching Security Threats

By Kenneth Corbin

CIO | Aug 8, 2014 4:47 AM PT

WASHINGTON – Security pros routinely cite poor cyber hygiene as one of their top concerns. But if they're lying awake at night worried about lazy passwords and software updates going ignored, just think of the headaches that will come once thermostats, pacemakers and just about everything else comes online.

When Randy Garrett contemplates the Internet of Things, he sees a colossal security challenge.

Garrett, a program manager at the Defense Advanced Research Projects Agency (DARPA), worries that, in the exuberance to embed sensors in a galaxy of devices and bring them onto the network, backers of the Internet of Things will unwittingly create a virtually limitless set of new threat vectors.

"This is where I think, frankly, we're already in trouble," Garrett said Wednesday at a conference on the Internet of Things. "You might not want to expose those to the big Internet."

He points to an array of security concerns that could arise in a thoroughly networked world. Chief among them is that – as uneven or just plain bad as the habits of PC users may be – many people are at least aware that the threats are out there and will often exercise some restraint in not clicking on spam links or avoid setting their password to "password."

Will Ability to Gather Data Trump Security Concerns?

Put another way, people recognize that there are malicious actors out there working to infiltrate their computers and swipe their personal information. But who thinks about their toaster in those terms?

It's not an idle concern. Recall the massive data breach Target sustained last year, exposing millions of the retailer's customers' information, forcing the Target CIO to step down and causing untold damage to the company brand.

The reported culprit? An entry point to the company's most sensitive data assets gained from a contractor who worked on Target's heating and air conditioning systems. "Who thought it was a good idea to connect that to the Internet?" Garrett asks.

Garrett's security concerns notwithstanding, there are strong arguments in favor of networking objects so they can be deployed more efficiently and monitored remotely.

Boosters of the Internet of Things can make a long list of areas where operations and safety could be improved by a networked set of smart devices. Household appliances could modulate

their power consumption to avoid peak load times. Sensors placed along railroad lines could relay temperature data that could help preempt track failures. The same could be done for bridges, tunnels and other pieces of the nation's fraying infrastructure.

A pilot project in Rockville, Md., for example, placed 14 sensors into an apartment building that monitor for smoke, heat, carbon monoxide and other potential danger signs, relaying them to a cloud service that dispatches emergency responders if a problem is observed.

Internet of Things Poised to Change (and Challenge) Healthcare, Retail

One of the most enticing applications of a network of far-flung sensors can be found in healthcare, where an entire industry is taking shape to build devices and applications with which patients can engage to monitor glucose levels, blood pressure or heart health, or perform any number of other diagnostic procedures and then relay the information back to a care provider.

"That's a much better set of data in which to diagnose and manage diseases," says Michael Chui, a partner and senior fellow at the McKinsey Global Institute.

Chui acknowledges a host of unknowns, security and otherwise, which arise with bringing physical objects online. Who is named in the lawsuit when two driverless cars are involved in an accident, he wonders.

At least in part, however, he suggests that some challenges, and solutions, could be found in a rethinking of organizations and their traditional roles and processes.

In a retail environment, for instance, the CIO's involvement in store operations might be limited to the cash registers, point-of-sale systems and back-office operations. In a world where mobile payments are a reality and items on the shelf are expected to interact with shoppers' devices, though, the tech team must take a more hands-on role.

"If that's the case, then the people managing IT actually have to touch the merchandise in a way that the store manager never would have wanted before," says Chui, who earlier in his career served as a municipal CIO. Likewise, in the military, he asks: "Does the CIO of the Army have to touch the tanks?"

"It's a tremendous number of organizational challenges when you start integrating the physical world with the virtual world, Chui adds. “You have to change the way you make decisions if you're going to use the Internet of things effectively."

IoT Devices Easily Hacked to be Backdoors: Experiment

By SecurityWeek News on January 13, 2016

Many consumer-grade Internet of Things (IoT) products, such as Wi-Fi security web cameras, include security flaws that allow attackers to reprogram them and use them as persistent backdoors, Vectra Networks warns.

According to the security firm, which focuses on detection of cyber-attacks, insecure IoT devices enable potential attackers to remotely command and control an attack while avoiding detection from traditional security products. By turning an IoT device into a backdoor, attackers gain 24x7 access to an organization's network without infecting a laptop, workstation or server, which are usually protected by firewalls, intrusion prevention systems and antivirus software.

While such security issues with IoT devices have been widely known for years, Vectra conducted an experiment that again shows the risks associated with adding them to your network.

The Vectra Threat Labs experiment focused on a popular D-Link Wi-Fi camera available for purchase at around $30. The security researchers managed to successfully reprogram it to act as a network backdoor without disrupting its operation as a camera, though the process required physical access to the device.

The researchers explain in a blog post that the reprogramming process started with taking the camera apart and dumping the content of the flash memory chip on the PCB (printed circuit board) for further analysis. The firmware was found to consist of a u-boot and a Linux kernel and image, and the team managed to access the Linux image filesystem.

After further analysys, the researchers decided to include the backdoor in the firmware in the form of a service inside the Linux system, and they went for a simple connect-back Socks proxy.

The team then tested whether they could bring back a telnet socket to an outside host, thus gaining remote persistence to the webcam. Having the webcam acting as a proxy allowed them to send control traffic into the

network to advance attacks and explains that an attacker could use the webcam to siphon out stolen data from a company's network.

However, the researchers also explain that this doesn't necessarily mean that D-Link's web camera has a major security issue, but that IoT devices have a high impact on the attack surface of a network. These devices can be hacked relatively easily and, while they do not cost that much, they certainly matter to the security of a network.

"Consumer-grade IoT products can be easily manipulated by an attacker, used to steal an organization's private information, and go undetected by traditional security solutions. While many of these devices are low-value in terms of hard costs, they can affect the security and integrity of the network, and teams need to keep an eye on them to reveal any signs of malicious behavior," Gunter Ollmann, CSO of Vectra Networks, said.

The security researchers also note that the security vulnerability was brought to D-Link's attention in early December 2015. However, the tech company hasn't provided a fix for the issue as of January 7, 2016.

As Rafal Los, director of solutions research and development within the Office of the CISO for Optiv, explains in a SecurityWeek column, many of these IoT devices (even secured and not hacked) are always-on, always connected, which could pose a privacy risk to end-users and a security risk to companies, if they are brought at the office. After all, companies might not have a policy for bringing IoT devices, although they might have BYOD policies in place.

The IoT market is expanding at a fast pace at the moment, and both security researchers and cybercriminals are increasingly focused on finding security flaws in devices that are considered as being part of this segment. The industry joined hands last year and launched the Internet of Things Security Foundation (IoTSF) in September to address concerns regarding the security of IoT devices.

In November 2015, security researchers presented at the DefCamp conference in Bucharest the findings of a study on the firmware of IoT devices, explaining that such firmware images are often susceptible to multiple security flaws because manufacturers do not properly test them for security flaws. Also in November, IT security consultancy SEC Consult

revealed that millions of IoT devices use the same cryptographic secrets, which expose them to various malicious attacks.

“Now is a great time to start to think about policy and procedure for the inevitable,” Los said. “As everything imaginable starts to ask for an IP address from your network, make sure you watch ingress and egress points and terminate encryption so you can properly inspect all traffic. What is your policy for things like the Amazon Echo, on your corporate network? Would your network even notice if one of these devices showed up, plugged in and pulled an IP address? Then what?”

Researchers Hope This Invention Could Wave Away Medical Data Hacks

May 10, 201612:10 PM ET

Jordan Gass-Pooré

Doctors' scrawls on prescription pads and medical folders are so analog.

These days, they're prescribing and keeping track of patients' records using digital devices connected to wireless networks, sometimes remotely. More medical devices are also becoming increasingly small and wearable; they often connect with a hand-held controller or even your smartphone through Bluetooth or Wi-Fi, sometimes sending the data directly to physicians.

This convenience, accessibility and cost reduction for our health care comes with risks. A few keystrokes could end in a wrong treatment, for instance — in 2007, Dick Cheney's cardiologist disabled the wireless functionality of the former vice president's heart defibrillator out of safety concerns.

The overarching and long-growing problem is this: How do we protect the highly personal data flowing through wirelessly connected medical devices?

Enter Wanda, a prototype developed by Dartmouth College doctoral student Timothy Pierson and his team.

Wanda is essentially two antennas attached to a ruler, in a wandlike fashion. The device uses radio waves to establish a secure wireless connection between devices that generate data.

Here's how it works: The user turns on the medical device and the digital device it's getting linked to and then points Wanda — about 11 inches or less away — at the devices one at a time. Wanda then generates and transmits a secret password to each of the devices, connecting them securely within seconds.

Many Wi-Fi networks that transmit personal data aren't secure connections — and cybercriminals make more money hacking a person's medical information than from stealing his credit card details, says David Kotz, a Dartmouth computer science professor who leads the Trustworthy Health and Wellness project. It's developing a technology platform that secures and protects personal health information.

Plus, putting these devices in the hands of patients and relying on them to establish Wi-Fi networks is fraught with difficulties. Some patients don't have the technical know-how; others have a medical condition that poses a challenge. Most people, however, just create security passwords for their Wi-Fi networks that can easily be hacked, Pierson says.

This could lead to a data breach that may compromise the security of a patient's records, or even the patient's health if, for instance, the wireless heart pacemaker or dialysis machine is hacked. Internet security experts have warned for years that these devices are open to data theft and remote control by hackers — and the equipment to do so cost less than $20 in 2011, when a researcher hacked into his insulin pump and altered the settings.

Wanda's major appeal is its ability to generate a targeted, strong pass code that connects a medical device in essence without the patient's involvement. Researchers elsewhere have tried similar hypothetical approaches, but they require extra equipment to be included in the medical device, Pierson says.

Some of these ideas suggest that a secret password can be created by using a speaker and a microphone to send sound waves to devices, or by simultaneously shaking devices equipped with accelerometers that detect motion and orientation to establish a secure wireless connection.

Try shaking a treadmill or a refrigerator, Pierson says. "We haven't seen anything like [Wanda] on the market," he adds.

Pierson says he and his colleagues envision possibilities for Wanda beyond health care, especially as more of our household items get connected to the Internet. But for now, the team's focus is on Wanda's ability to protect sensitive patient data in a medical setting.

Wanda for now is only a prototype. Pierson says it has been received well by volunteer testers who have expressed interest in purchasing the device if and when it hits the market. A release date hasn't been scheduled because Pierson and his team are still in the process of filing for a patent.

The Senate health committee has been working on legislation that may help spur these kinds of devices through federal regulatory approvals. The lawmakers have set data security as a priority in their latest biomedical innovation agenda.

Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent

Scott R. Peppet*

The consumer "Internet of Things" is suddenly reality, not science fiction. Electronic sensors are now ubiquitous in our smartphones, cars, homes, electric systems, health-care devices, fitness monitors, and workplaces. These connected, sensor-based devices create new types and unprecedented quantities of detailed, high-quality information about our everyday actions, habits, personalities, and preferences. Much of this undoubtedly increases social welfare. For example, insurers can price automobile coverage more accurately by using sensors to measure exactly how you drive (e.g., Progressive's Snapshot system), which should theoretically lower the overall cost of insurance. But the Internet of Things raises new and difficult questions as well. This Article shows that four inherent aspects of sensor-based technologies—the compounding effects of what computer scientists call "sensor fusion," the near impossibility of truly de-identifying sensor data, the likelihood that Internet of Things devices will be inherently prone to security flaws, and the difficulty of meaningful consumer consent in this context—create very real discrimination, privacy, security, and consent problems. As connected, sensor-based devices tell us more and more about ourselves and each other, what discrimination—racial, economic, or otherwise—will that permit, and how should we constrain socially obnoxious manifestations? As the Internet of Things generates ever more massive and nuanced datasets about consumer behavior, how to protect privacy? How to deal with the reality that sensors are particularly vulnerable to security risks? How should the law treat—and how much should policy depend upon—consumer consent in a context in which true informed choice may be impossible? This Article is the first legal work to describe the new connected world we are creating, address these four interrelated problems, and propose concrete first steps for a regulatory approach to the Internet of Things.

INTRODUCTION 87
I. THE INTERNET OF THINGS 98
A. Health & Fitness Sensors 98
1. Countertop Devices 99
2. Wearable Sensors 100
3. Intimate Contact Sensors 102
4. Ingestible & Implantable Sensors 103

* Professor of Law, University of Colorado School of Law. I am grateful to the faculty of the University of Colorado Law School for their input, and particularly to Paul Ohm and Harry Surden for their thoughts. I also thank the participants at the Federal Trade Commission's Internet of Things Workshop (November 19, 2013), who gave helpful comments on many of these ideas. Finally, thank you to my research assistants Carey DeGenero and Brian Petz for their help.

B. Automobile Sensors 104
1. Event Data Recorders 104
2. Consumer Automobile Sensors 104
3. Auto-Insurance Telematics Devices 106
C. Home & Electricity Sensors 108
1. The Smart Home 108
2. The Smart Grid 109
D. Employee Sensors 111
E. Smartphone Sensors 114
II. FOUR PROBLEMS 117
A. Discrimination 117
1. The Technical Problem: Sensor Fusion & Big Data Analytics May Mean That Everything Reveals Everything 118
2. The Legal Problem: Antidiscrimination and Credit Reporting Law Is Unprepared 123
a. Racial & Other Protected Class Discrimination 123
b. Economic Discrimination 125
B. Privacy 128
1. The Technical Problem: Sensor Data Are Particularly Difficult to De-Identify 128
2. The Legal Problem: Privacy Law Is Unprepared 131
C. Security 132
1. The Technical Problem: Internet of Things Devices May Be Inherently Prone to Security Flaws 133
2. The Legal Problem: Data Security Law Is Unprepared 135
D. Consent 139
1. The Technical Problem: Sensor Devices Confuse Notice and Choice 139
a. The Difficulties with Finding Internet of Things Privacy Policies 139
b. The Ambiguity of Current Internet of Things Privacy-Policy Language 142
c. The Glaring Omissions from Internet of Things Privacy Policies 144
2. The Legal Problem: Consumer Protection Law Is Unprepared 145
III. FOUR (MESSY & IMPERFECT) FIRST STEPS 147
A. A Regulatory Blueprint for the Internet of Things 149
1. Dampening Discrimination with Use Constraints 149
a. Cross-Context Use Constraints 150
b. Constraints on Forced Disclosure Even Within a Given Context 152
2. Protecting Privacy by Redefining Personally Identifiable Information in This Context 155
3. Protecting Security by Expanding Data-Breach Notification Laws 157
4. Improving Consent by Guiding Internet of Things

Consumer Disclosures 159
B. Seize the Moment: Why Public Choice Problems Demand Urgency 163
CONCLUSION 164
APPENDIX 165

> [E]very animate and inanimate object on Earth will soon be *generating data*, including our homes, our cars, and yes, even our bodies.[1]
>
> —Anthony D. Williams, in *The Human Face of Big Data* (2012)

> Very soon, we will see inside ourselves like never before, with wearable, even internal[,] sensors that monitor even our most intimate biological processes. It is likely to happen even before we figure out the etiquette and laws around sharing this knowledge.[2]
>
> —Quentin Hardy, *The New York Times* (2012)

> [A]ll data is credit data, we just don't know how to use it yet. . . . Data matters. More data is always better.[3]
>
> —Douglas Merrill, Google's former CIO & CEO of ZestFinance

Introduction

The Breathometer is a small, black plastic device that plugs into the headphone jack of an Android or iPhone smartphone.[4] Retailing for $49, the unit contains an ethanol sensor to estimate blood alcohol content from the breath.[5] The company's website advertises that the device will give you "the power to make smarter decisions when drinking."[6] The device works only in conjunction with the downloadable Breathometer application (app),

---

1. RICK SMOLAN & JENNIFER ERWITT, THE HUMAN FACE OF BIG DATA (2012) (paraphrasing Anthony D. Williams, *Science's Big Data Revolution Yields Lessons for All Open Data Innovators*, ANTHONYDWILLIAMS (Mar. 30, 2011), http://anthonydwilliams.com/2011/03/30/sciences-big-data-revolution-yields-lessons-for-all-open-data-innovators/, *archived at* http://perma.cc/6JP-P2WE).

2. Quentin Hardy, *Big Data in Your Blood*, BITS, N.Y. TIMES (Sept. 7, 2012, 10:37 AM), http://bits.blogs.nytimes.com/2012/09/07/big-data-in-your-blood/?_php=true&_type=blogs&_r=0, *archived at* http://perma.cc/45EZ-9LY5.

3. Quentin Hardy, *Just the Facts. Yes, All of Them.*, N.Y. TIMES, Mar. 24, 2012, http://www.nytimes.com/2012/03/25/business/factuals-gil-elbaz-wants-to-gather-the-data-universe.html?pagewanted=all, *archived at* http://perma.cc/665S-7YWX; *see also How We Do It*, ZESTFINANCE, http://www.zestfinance.com/how-we-do-it.html, *archived at* http://perma.cc/WY59-9EFW (touting the firm's philosophy that "All Data is Credit Data").

4. BREATHOMETER™, http://www.breathometer.com, *archived at* http://perma.cc/E88P-2JTT.

5. *Frequently Asked Questions*, BREATHOMETER™, https://www.breathometer.com/help/faq, *archived at* http://perma.cc/HJL8-6VE8.

6. *See* BREATHOMETER™, *supra* note 4.

which both displays the results of any given test and shows a user's longitudinal test history.

The Breathometer is representative of a huge array of new consumer devices promising to measure, record, and analyze different aspects of daily life that have exploded onto the market in the last twelve to eighteen months.[7] For example, a Fitbit bracelet or Nike+ FuelBand can track the steps you take in a day, calories burned, and minutes asleep; a Basis sports watch will track your heart rate; a Withings cuff will graph your blood pressure on your mobile phone or tablet; an iBGStar iPhone add-on will monitor your blood glucose levels; a Scanadu Scout will measure your temperature, heart rate, and hemoglobin levels; an Adidas miCoach Smart Ball will track your soccer performance;[8] a UVeBand or JUNE bracelet will monitor your daily exposure to ultraviolet rays and notify your smartphone if you need to reapply sunscreen;[9] a Helmet by LifeBEAM will track your heart rate, blood flow, and oxygen saturation as you cycle; a Mimo Baby Monitor "onesie" shirt will monitor your baby's sleep habits, temperature, and breathing patterns; a W/Me bracelet from Phyode will track changes in your autonomic nervous system to detect mental state (e.g., passive, excitable, pessimistic, anxious, balanced) and ability to cope with stress;[10] and a Melon or Muse headband can measure brain activity to track your ability to focus.[11] Other devices—such as the popular Nest Thermostat; SmartThings' home-automation system; the Automatic Link driving and automobile monitor; GE's new line of connected ovens, refrigerators, and other appliances; and Belkin's WeMo home electricity and water-usage tracker—can in combination measure your driving habits, kitchen-appliance use, home electricity and water consumption, and even work productivity.[12]

7. For a more thorough description of each of these devices, please see *infra* subparts I(A)–(E).

8. *MiCoach Smart Ball*, ADIDAS, http://micoach.adidas.com/smartball/, *archived at* http://perma.cc/W9A7-5GG9.

9. *How to Use the UveBand*, UVEBAND, http://suntimellc.com/?page_id=12, *archived at* http://perma.cc/6UR6-5AAM; JUNE, NETATMO, https://www.netatmo.com/en-US/product/june, *archived at* http://perma.cc/K4BS-SVYC.

10. *W/Me*, PHYODE, http://www.phyode.com/health-wristband.html, *archived at* http://perma.cc/VV34-LA47.

11. MELON, http://www.thinkmelon.com/, *archived at* http://perma.cc/68DN-J3K8; *Frequently Asked Questions*, MUSE™, http://www.choosemuse.com/pages/faq#general, *archived at* http://perma.cc/KRA5-8DH9.

12. *See infra* subparts I(A)–(E).

Together these devices create the Internet of Things,[13] or what some have more recently called the "Internet of Everything."[14] Conservative estimates suggest that over 200 billion connected sensor devices will be in use by 2020,[15] with a market size of roughly $2.7 trillion to $6.2 trillion per year by 2025.[16] These devices promise important efficiency, social, and individual benefits through quantification and monitoring of previously immeasurable qualities. But the Internet of Things also raises a host of difficult questions. Who owns the data these sensors generate? How can such data be used? Are such devices, and the data they produce, secure? And are consumers aware of the legal implications that such data create—such as the possible use of such data by an adversary in court, an insurance company when denying a claim, an employer determining whether to hire, or a bank extending credit?

Return to the Breathometer example. When you purchase a Breathometer—as I did recently for purposes of researching this Article—it arrives in a small, stylish black box featuring an image of the device and the motto "Drink Smart. Be Safe." Opening the packaging reveals both the device and a small user's manual that explains how to download the Breathometer app, create an account with the company through that app, and plug the Breathometer into one's smartphone. Nowhere in that manual's seventeen pages is there mention of a privacy policy that might apply to the data generated by the device. Nor is there an explanation of what data the device generates (e.g., "just" blood alcohol content or also other sensor

13. The term is generally attributed to Kevin Ashton. Thomas Goetz, *Harnessing the Power of Feedback Loops*, WIRED, June 19, 2011, http://www.wired.com/2011/06/ff_feedbackloop/, *archived at* http://perma.cc/H9D3-V6D3; *see* Kevin Ashton, *That 'Internet of Things' Thing*, RFID J., June 22, 2009, http://www.rfidjournal.com/articles/pdf?4986, *archived at* http://perma.cc/B4CW-M29Z (claiming that the first use of the term "Internet of Things" was in a 1999 presentation by Ashton). *See generally* NEIL GERSHENFELD, WHEN THINGS START TO THINK (1999) (addressing the general concept of merging the digital world with the physical world); Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, 1 J. SENSOR & ACTUATOR NETWORKS 217 (2012) (exploring various ways of defining and characterizing the Internet of Things and assessing its features, limitations, and future).

14. The phrase "Internet of Everything" seems to originate with Cisco's CEO John Chambers. *See* Robert Pearl, *Cisco CEO John Chambers: American Health Care Is at a Tipping Point*, FORBES (Aug. 28, 2014, 1:00 PM), http://www.forbes.com/sites/robertpearl/2014/08/28/cisco-ceo-john-chambers-american-health-care-is-at-a-tipping-point/, *archived at* http://perma.cc/XET3-D37A (quoting Chambers that the "Internet of Everything" brings "people, process, data and things" together in order to make "connections more relevant and valuable than ever before"); *cf. Frequently Asked Questions*, *The Internet of Everything: Cisco IoE Value Index Study*, CISCO, http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe-value-index_FAQs.pdf, *archived at* http://perma.cc/Y4LQ-633J (reiterating Cisco's definition of the Internet of Everything as "the networked connection of people, process, data, and things").

15. Tim Bajarin, *The Next Big Thing for Tech: The Internet of Everything*, TIME, Jan. 13, 2014, http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything, *archived at* http://perma.cc/79RK-BDCY.

16. JAMES MANYIKA ET AL., MCKINSEY & CO., DISRUPTIVE TECHNOLOGIES: ADVANCES THAT WILL TRANSFORM LIFE, BUSINESS, AND THE GLOBAL ECONOMY 51 (2013).

information?); where such data are stored (e.g., in one's phone or on the company's servers in the cloud?); whether such data can be deleted and how; or how the company might use such data (e.g., will the company sell it; could it be subpoenaed through a court process?). When installing the Breathometer app through the Apple App Store, no mention is made of any privacy policy. No pop-up with such a policy appears when the user creates an account through the app or starts using the device. In short, the data-related aspects of the device are completely absent from the user experience. Only by visiting the company's website, scrolling to the very bottom, and clicking the small link for "Privacy Policy" can one learn that one's blood-alcohol test results are being stored indefinitely in the cloud, cannot be deleted by the user, may be disclosed in a court proceeding if necessary, and may be used to tailor advertisements at the company's discretion.[17]

Given the many potentially troubling uses for breathalyzer data—think employment decisions; criminal liability implications; and health, life, or car-insurance ramifications—one might expect data-related disclosures to dominate the Breathometer user's purchasing and activation experience. Instead, the consumer is essentially led to the incorrect assumption that this small black device is merely a good like any other—akin to a stapler or ballpoint pen—rather than a data source and cloud-based data repository.[18]

Even Internet of Things devices far more innocuous than the Breathometer can generate data that present difficult issues. Sensor data capture incredibly rich nuance about who we are, how we behave, what our tastes are, and even our intentions. Once filtered through "Big Data" analytics,[19] these data are the grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities. I can tell a lot about you if I know that you often leave your oven on when you leave the house, fail to water your plants, don't exercise, or drive recklessly.[20] As Federal Trade Commission (FTC) Commissioner Julie Brill recently stated:

> On the Internet of Things, consumers are going to start having devices, whether it's their car, or some other tool that they have, that's connected and sending information to a number of different entities, and the consumer might not even realize that they have a connected

17. *Privacy Policy*, BREATHOMETER™ [hereinafter *Privacy Policy*, BREATHOMETER™], http://www.breathometer.com/legal/privacy-policy, *archived at* http://perma.cc/T7BW-S7R3.

18. *See* ADRIAN MCEWEN & HAKIM CASSIMALLY, DESIGNING THE INTERNET OF THINGS 294 (2014) ("[M]any 'things' have little in their external form that suggests they are connected to the Internet. When you grab an Internet-connected scarf from the coat rack or sit on an Internet-connected chair, should you have some obvious sign that data will be transmitted or an action triggered?"); *Privacy Policy*, BREATHOMETER™, *supra* note 17 (emphasizing that mere use of a Breathometer operates as acceptance of the privacy policy).

19. *See generally* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239 (2013) (explaining how advances in data analytics that broaden the scope of information available to third parties have accompanied the increase in the number of individuals, devices, and sensors connected by digital networks).

20. *See infra* Part I.

> device or that the thing that they're using is collecting information about them.[21]

These are the real challenges of the Internet of Things: what information do these devices collect, how might that information be used, and what—if any—real choice do consumers have about such data?

To date, the law has left these questions unanswered. Consider a second preliminary example. Roughly ninety percent of new automobiles in the United States contain an Event Data Recorder (EDR) or "black box."[22] By federal law, such devices must store a vehicle's speed, how far the accelerator pedal is pressed, whether the brake is applied, whether the driver is using a seat belt, crash details, and other information, including, in some cases, the driver's steering input and occupant sizes and seat positions.[23] Such data can convict unsafe drivers[24] and help regulators improve safety,[25] but many policy questions remain unanswered or only partially addressed. Can an insurance company, for example, require an insured *ex ante* to grant access to EDR data in the insured's policy or condition *ex ante* claim payment on such access? The National Highway Traffic Safety Administration (NHTSA) has left who owns EDR data—the car owner, the manufacturer, or the insurer—to the states,[26] but only fourteen states have addressed the issue.[27] Four states currently forbid insurance companies from requiring that an insured consent to future disclosure of EDR data or from requiring access

---

21. Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the Silicon Flatirons Conference: The New Frontiers of Privacy Harm (Jan. 17, 2014), *available at* http://youtu.be/VXEyKGw8wXg, *archived at* http://perma.cc/F335-E987.

22. *See* Press Release, Nat'l Highway Traffic Safety Admin., U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety (Dec. 7, 2012), *available at* http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Safety, *archived at* http://perma.cc/963A-F72E ("NHTSA estimates that approximately 96 percent of model year 2013 passenger cars and light-duty vehicles are already equipped with EDR capability."). The NHTSA's 2012 estimate represented a nearly 30% increase from the estimated number of EDRs in new-model cars in 2004. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., FINAL REGULATORY EVALUATION: EVENT DATA RECORDERS (EDRS), at III-2 tbl.III-1 (2006) (estimating that 64.3% of new cars sold in 2004 came equipped with EDRs).

23. Event Data Recorders Rule, 49 C.F.R. § 563.7 (2013).

24. *See* Matos v. Florida, 899 So. 2d 403, 407 (Fla. Dist. Ct. App. 2005) (holding that data from certain EDRs are admissible when used as tools for automotive accident reconstruction).

25. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., DOCKET NO. NHTSA-1999-5218-0009, EVENT DATA RECORDERS: SUMMARY OF FINDINGS BY THE NHTSA EDR WORKING GROUP 67 (2001), *available at* http://www.regulations.gov/#!documentDetail;D=NHTSA-1999-5218-0009, *archived at* http://perma.cc/X5SK-2SDK (finding that EDR data may be used for various real-world safety applications, including collision avoidance, occupant protection, and roadside safety monitoring).

26. Event Data Recorders, 71 Fed. Reg. 50,998, 51,030 (Aug. 28, 2006) (to be codified at 49 C.F.R. pt. 563).

27. *Privacy of Data from Event Data Recorders: State Statutes*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx, *archived at* http://perma.cc/7XRZ-TNZ7.

to EDR data as a condition of settling an insurance claim.[28] One state—Virginia—also forbids an insurer from adjusting rates solely based on an insured's refusal to provide EDR data.[29] Should other states follow? Should Congress give federal guidance on such uses of EDR data? Is such fine-grained information invasive of privacy—particularly given that consumers cannot easily turn off or "opt out" of its collection? And as more sophisticated car sensors reveal even more sensitive information—where we drive, when we drive, how we drive—that permits deeper inferences about us—how reckless, impulsive, or quick to anger we are—how will we regulate the use of such data? For example, should a bank be able to deny your mortgage application because your EDR data reveal you as an irresponsible driver and, thus, a bad credit risk? Should a potential employer be able to factor in a report based upon your driving data when deciding whether to hire you?

In beginning to answer these questions, this Article makes three claims about the Internet of Things—all new to the legal literature, all important, and all timely.

First, the sensor devices that together make up the Internet of Things are not a science-fiction future but a present reality. Internet of Things devices have proliferated before we have had a chance to consider whether and how best to regulate them. Sales of fitness trackers such as Fitbit and Nike+ FuelBand topped $300 million last year, and consumer sensor devices dominated the January 2014 International Consumer Electronics Show.[30] The hype is real: such devices are revolutionizing personal health, home security and automation, business analytics, and many other fields of human activity. The scant legal work addressing such devices has largely assumed, however, that the Internet of Things is still in its infancy in a research laboratory, not yet ready for commercial deployment at scale.[31] To counter this misperception and lay the foundation for considering the current legal problems created by the Internet of Things, Part I presents a typology of consumer sensors and provides examples of the myriad ways in which existing Internet of Things devices generate data about our environment and our lives.

Second, the Internet of Things suffers from four unique technical challenges that in turn create four legal problems concerning discrimination, privacy, security, and consent. This is the heart of the Article's argument, and it is the four-pronged focus of Part II.

---

28. *See infra* note 397.

29. *See infra* note 398.

30. Jonah Comstock, *In-depth: The MobiHealthNews CES 2014 Wrap-Up*, MOBIHEALTHNEWS (Jan. 17, 2014), http://mobihealthnews.com/28689/in-depth-the-mobihealthnews-ces-2014-wrap-up/, *archived at* http://perma.cc/F9A6-APYN.

31. *See, e.g.*, Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 815–17 (2012) (describing the use of self-surveillance devices and sensors but focusing primarily on laboratory and experimental contexts rather than commercial context).

First, subpart II(A) explores the ways in which the Internet of Things may create new forms of discrimination—including both racial or protected class discrimination and economic discrimination—by revealing so much information about consumers. Computer scientists have long known that the phenomenon of "sensor fusion" dictates that the information from two disconnected sensing devices can, when combined, create greater information than that of either device in isolation.[32] Just as two eyes generate depth of field that neither eye alone can perceive, two Internet of Things sensors may reveal unexpected inferences. For example, a fitness monitor's separate measurements of heart rate and respiration can in combination reveal not only a user's exercise routine, but also cocaine, heroin, tobacco, and alcohol use, each of which produces unique biometric signatures.[33] Sensor fusion means that on the Internet of Things, "every thing may reveal everything." By this I mean that each type of consumer sensor (e.g., personal health monitor, automobile black box, or smart grid meter) can be used for many purposes beyond that particular sensor's original use or context, particularly in combination with data from other Internet of Things devices. Soon we may discover that we can infer whether you are a good credit risk or likely to be a good employee from driving data, fitness data, home energy use, or your smartphone's sensor data.

This makes each Internet of Things device—however seemingly small or inconsequential—important as a policy matter, because any device's data may be used in far-removed contexts to make decisions about insurance, employment, credit, housing, or other sensitive economic issues. Most troubling, this creates the possibility of new forms of racial, gender, or other discrimination against those in protected classes if Internet of Things data can be used as hidden proxies for such characteristics. In addition, such data may lead to new forms of economic discrimination as lenders, employers, insurers, and other economic actors use Internet of Things data to sort and treat differently unwary consumers. Subpart II(A) explores the problem of discrimination created by the Internet of Things, and the ways in which both traditional discrimination law and privacy statutes, such as the Fair Credit Reporting Act (FCRA),[34] are currently unprepared to address these new challenges.

Subpart II(B) considers the privacy problems of these new technologies. The technical challenge here is that Internet of Things sensor data are particularly difficult to de-identify or anonymize. The sensors in Internet of

32. *See infra* notes 226–29 and accompanying text.

33. *See generally, e.g.*, Annamalai Natarajan et al., *Detecting Cocaine Use with Wearable Electrocardiogram Sensors*, *in* UBICOMP'13: PROCEEDINGS OF THE 2013 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING 123, 123 (2013) (hypothesizing that cocaine use can reliably be detected using electrocardiogram (ECG) sensor data and supporting this hypothesis through a clinical study conducted using ECG readings from a commercially available device, the Zephyr BioHarness 3).

34. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012).

Things devices often have entirely unique "fingerprints"—each digital camera, for example, has its own signature imperfections and irregularities.[35] Moreover, even when identifying characteristics such as name, address, or telephone number are removed from Internet of Things datasets, such sensor data are particularly vulnerable to re-identification. A recent MIT study showed, for example, that it is far easier than expected to re-identify "anonymized" cell-phone users, and other computer-science work has likewise shown that Internet of Things sensor devices are particularly prone to such attacks.[36] Unfortunately, privacy law is not prepared to deal with this threat of easy re-identification of Internet of Things information and instead relies on the outdated assumption that one can usefully distinguish between "personally identifiable information" and de-identified sensor or biometric data. Subpart II(B) shows that this may no longer be viable on the Internet of Things.

Subpart II(C) then turns to the unique data-security problems posed by the Internet of Things. The technical challenge is simple: many Internet of Things products have not been engineered to protect data security. These devices are often created by consumer-goods manufacturers, not computer software or hardware firms. As a result, data security may not be top of mind for current Internet of Things manufacturers. In addition, the small form factor and low power and computational capacity of many of these Internet of Things devices makes adding encryption or other security measures difficult. Recent attacks—such as a November 2013 attack that took control of over 100,000 Internet of Things web cameras, appliances, and other devices[37]—highlight the problem. Data-security researchers have found vulnerabilities in Fitbit fitness trackers, Internet-connected insulin pumps, automobile sensors, and other products.[38] Unfortunately, both current FTC enforcement practices and state data-breach notification laws are unprepared to address Internet of Things security problems. In particular, were Fitbit, Nike+ FuelBand, Nest Thermostat, or any other Internet of Things manufacturers to have users' sensitive sensor data stolen, *no* existing state data-breach notification law would currently require public disclosure or remedy of such a breach.[39]

Next, subpart II(D) considers the ways in which consumer protection law is also unprepared for the Internet of Things. In particular, I present the first survey in the legal literature of Internet of Things privacy policies and show the ways in which such policies currently fail consumers.[40] Internet of Things devices generally have no screen or keyboard, and thus giving

35. *See infra* note 268.
36. *See infra* notes 271–74 and accompanying text.
37. *See infra* notes 291–92 and accompanying text.
38. *See infra* section II(C)(1).
39. *See infra* section II(C)(2).
40. *See infra* subpart II(D) and Appendix.

consumers data and privacy information and an opportunity to consent is particularly challenging. Current Internet of Things products often fail to notify consumers about how to find their relevant privacy policy, and once found, such policies are often confusing, incomplete, and misleading. My review shows that such policies rarely clarify who owns sensor data, exactly what biometric or other sensor data a device collects, how such data are protected, and how such information can be sold or used. Both state and federal consumer protection law has not yet addressed these problems or the general issues that the Internet of Things creates for consumer consent.

Part II's focus on these four problems of discrimination, privacy, security, and consent concludes with a fairly dismal warning to regulators, legislators, privacy and consumer advocates, and corporate counsel: current discrimination, privacy, data security, and consumer protection law is unprepared for the Internet of Things, leaving consumers exposed in a host of ways as they begin to use these new devices. Absent regulatory action to reassure and protect consumers, the potential benefits of the Internet of Things may be eclipsed by these four serious problems.

Third, state and federal legislators and regulators should take four preliminary steps to begin to guide the Internet of Things. This argument—in Part III—is the Article's most difficult. I could easily prescribe a comprehensive new federal statute or the creation of a new oversight agency, but such approaches are simply implausible given current political realities. Vague prescriptions—such as calling for greater consumer procedural protections or due process—would also sound good without offering much immediate or practical progress. Yet real, operational prescriptions are challenging, in part because my goal in Part II is to provide a comprehensive map of the four major problems generated by the Internet of Things rather than focus on merely one aspect such as security or consent. Put simply, if Part II's description of the challenges we face is broad and accurate enough, proposing realistic prescriptions in Part III is necessarily daunting.

Nevertheless, Part III begins to lay out a regulatory blueprint for the Internet of Things. I take four prescriptive positions. First, new forms of discrimination will best be addressed through substantive restrictions on certain uses of data, not through promises to consumers of procedural due process. I therefore propose extending certain state laws that inhibit use of sensor data in certain contexts, such as statutes prohibiting insurers from conditioning insurance on access to automobile EDR data.[41] Although this approach is at odds with much information-privacy scholarship, I nevertheless argue that use constraints are necessary to prevent obnoxious discrimination on the Internet of Things. Second, biometric and other sensitive sensor data created by the Internet of Things should be considered potential personally identifiable information, even in supposedly de-

41. *See infra* section III(A)(1).

identified forms. I show how regulators and corporate counsel should therefore reconsider the collection, storage, and use of such data.[42] Third, we should at least protect sensor-data security by broadening state data-breach notification laws to include such data within their scope and create substantive security guidelines for Internet of Things devices. Although regulators may currently lack legislative authority to strictly enforce such guidelines, they nevertheless can use their "soft" regulatory power to create industry consensus on best practices for Internet of Things security.[43] Finally, we should rigorously pursue Internet of Things firms for promulgating incomplete, confusing, and sometimes deceptive privacy policies, and provide regulatory guidance on best practices for securing meaningful consumer consent in this difficult context.[44] Having shown in Part II the many ways in which notice and choice is currently failing on the Internet of Things, I suggest several concrete privacy-policy changes for regulators and corporate counsel to take up.

I do not pretend that these steps will solve every problem created by the Internet of Things. I aim to begin a conversation that is already overdue. Although some privacy scholarship has mentioned the proliferation of sensors,[45] none has systematically explored both the problems and opportunities the Internet of Things creates.[46] Some have explored particular contexts but not the complexity of the Internet of Things.[47] In a recent article,

---

42. *See infra* section III(A)(2).

43. *See infra* section III(A)(3).

44. *See infra* section III(A)(4).

45. *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1475–76 (2000) (predicting that no place on earth will be free from surveillance and monitoring as sensors and databases continue to proliferate); Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2322–24 (2007) (focusing primarily on cameras and surveillance rather than other, commercially available sensors). Much scholarship focused on other privacy issues at least mentions sensors. *See, e.g.*, Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936, 1940 (2013) (discussing government surveillance and the effects thereof on democratic society but also emphasizing that the Internet of Things will increasingly subject "previously unobservable activity to electronic measurement, observation, and control").

46. *See, e.g.*, Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93, 94–95 (2005) (endeavoring to examine the costs and benefits of pervasive computing—the ubiquitous overlay of computing elements onto physical and material environments—and doubting whether these costs and benefits have previously been adequately considered); Kang et al., *supra* note 31, at 812 (opining that the potential benefits of self-surveillance data may be outweighed by "substantial privacy costs"); Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 65, 72 (2008) (emphasizing that existing analytical methods for addressing privacy threats do not adequately address the new species of threats created by the "generative Net"). Some forthcoming scholarship is beginning to focus more granularly on the Internet of Things. *See generally, e.g.*, John Gudgel, Objects of Concern? Risks, Rewards and Regulation in the "Internet of Things" (Apr. 29, 2014) (unpublished manuscript), http://ssrn.com/abstract=2430780, *archived at* http://perma.cc/CYU9-LFTK (addressing the costs and benefits of the Internet of Things, analyzing the policy implications thereof, and advocating for a flexible regulatory approach).

47. *See, e.g.*, Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 165–74 (2013) (exploring the threats to privacy posed by smart grids and the communication of data between smart meters and electric utilities); Kevin L. Doran, *Privacy and*

I highlighted the increased use of such sensor data without offering analysis of how to address its proliferation.[48] Even computer science is just beginning to focus on the problems created by widespread use of consumer sensor devices,[49] as are regulators—the FTC recently held its first workshop on the Internet of Things to solicit input on the privacy problems sensors create and how to address such issues.[50] This Article begins to fill this gap.

Before we begin, let me highlight four things I am *not* focused upon here. First, I am not talking about industrial or commercial sensors deployed in factories, warehouses, ports, or other workspaces that are designed to keep track of machinery and production. This is an important part of the Internet of Things, but this Article focuses primarily on consumer devices. Second, I am not talking in general about ambient sensor devices used in an environment to capture information about the use of that space, such as temperature sensors. Such ambient informatics also create difficult privacy and regulatory issues, but those are beyond our scope here. Third, I am not talking about the government's use of sensor data and the constitutional issues that arise from such use. Future work will have to address how to deal with a governmental subpoena of Fitbit or whether the National Security Agency can or does track consumer sensor data.[51] Fourth, I am not talking about the privacy concerns that a sensor I am wearing might create for *you* as you interact with me. My sensor might sense and record your behavior, as when a cell phone's microphone records my speech but also yours, thus creating a privacy concern for you. Instead, here I focus on the issues raised

---

Smart Grid: When Progress and Privacy Collide, 41 U. TOL. L. REV. 909, 911–12 (2010) (examining the smart grid and related privacy concerns in regard to the Fourth Amendment and third-party doctrine); Karin Mika, *The Benefit of Adopting Comprehensive Standards of Monitoring Employee Technology Use in the Workplace*, CORNELL HR REV., Sept. 22, 2012, at 1, 1–2, http://www.cornellhrreview.org/wp-content/uploads/2012/09/Mika-Employer-Monitoring-2012.pdf, *archived at* http://perma.cc/934F-L8AF (considering electronic monitoring in an employer–employee relationship and proposing that employers devise effective policies that balance their interests against their employees' privacy interests); Patrick R. Mueller, Comment, *Every Time You Brake, Every Turn You Make—I'll Be Watching You: Protecting Driver Privacy in Event Data Recorder Information*, 2006 WIS. L. REV. 135, 138–39 (discussing event data recorders in vehicles and the lack of privacy protections for individuals and proposing a legislative solution).

48. *See* Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1167–73 (2011) (providing examples of digital monitoring of data in "health care, equipment tracking, and employee monitoring").

49. *See, e.g.*, Andrew Raij et al., *Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment*, *in* CHI 2011: PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 11, 11 (2011) ("[L]ittle work has investigated the new privacy concerns that emerge from the disclosure of measurements collected by wearable sensors.").

50. *Internet of Things–Privacy and Security in a Connected World*, FED. TRADE COMMISSION, http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world, *archived at* http://perma.cc/GW2Y-2LEY.

51. *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 556 (2012) (criticizing the inadequacy of current statutory and jurisprudential frameworks for evaluating government biometric-identification initiatives).

for users themselves. Each of these other problems is a worthwhile topic for future work.

I. The Internet of Things

Microelectromechanical systems (MEMS) sensors translate physical phenomenon, such as movement, heat, pressure, or location, into digital information.[52] MEMS were developed in the 1980s, but in the last few years the cost of such sensors has dropped from twenty-five dollars to less than a dollar per unit.[53] These sensors are thus no longer the stuff of experimental laboratories; they are incorporated into consumer products available at scale. Some estimate that by 2025 over one *trillion* sensor-based devices will be connected to the Internet or each other.[54]

Part I aims to describe the Internet of Things technologies currently available to consumers. It overviews five types of Internet of Things devices: health and fitness sensors, automobile black boxes, home monitors and smart grid sensors, devices designed specifically for employee monitoring, and software applications that make use of the sensors within today's smartphones. Together, these consumer products fundamentally change our knowledge of self, other, and environment.

A. Health & Fitness Sensors

There are five basic types of personal health monitors, in order from least physically invasive to most invasive: (1) countertop devices (such as a blood-pressure monitor or weight scale); (2) wearable sensors (such as an arm or wrist band); (3) intimate contact sensors (such as a patch or electronic tattoo); (4) ingestible sensors (such as an electronic pill); and (5) implantable sensors (such as a heart or blood health monitor).[55] Each is already deployed commercially, and the market for health and wellness sensors has exploded in the last twelve to eighteen months. Mobile health-care and medical app downloads are forecast to reach 142 million in 2016, up from 44 million in

52. A sensor is defined as "a device that receives a stimulus and responds with an electrical signal." JACOB FRADEN, HANDBOOK OF MODERN SENSORS 2 (4th ed. 2010) (emphasis omitted).

53. Alexander Wolfe, *Little MEMS Sensors Make Big Data Sing*, ORACLE *VOICE*, FORBES (June 10, 2013, 10:26 AM), http://www.forbes.com/sites/oracle/2013/06/10/little-mems-sensors-make-big-data-sing/2/, *archived at* http://perma.cc/7S6E-HQL7.

54. Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, WIRED, May 14, 2013, http://www.wired.com/2013/05/internet-of-things-2/all/, *archived at* http://perma.cc/8EM3-VKP9.

55. *See* D. Konstantas, *An Overview of Wearable and Implantable Medical Sensors*, *in* IMIA YEARBOOK OF MEDICAL INFORMATICS 2007: BIOMEDICAL INFORMATICS FOR SUSTAINABLE HEALTH SYSTEMS 66, 67–69 (A. Geissbuhler et al. eds., 2007) (describing sensor-filled clothing, patch sensors, and implantable sensors); George Skidmore, *Ingestible, Implantable, or Intimate Contact: How Will You Take Your Microscale Body Sensors?*, SINGULARITYHUB (May 13, 2013, 8:43 AM), http://singularityhub.com/2013/05/13/ingestible-implantable-or-intimate-contact-how-will-you-take-your-microscale-body-sensors/, *archived at* http://perma.cc/6SCJ-H986 (cataloging the various uses and methodologies of implantable, ingestible, and intimate contact sensors).

2012,[56] creating a market worth $26 billion by 2017.[57] Almost 30 million wireless, wearable health devices—such as Fitbit or Nike+ FuelBand—were sold in 2012, and that figure was expected to increase to 48 million in 2013.[58]

1. Countertop Devices.—Countertop devices include weight scales, blood-pressure monitors, and other products meant to be used occasionally to track some aspect of health or fitness. The Aria and Withings scales, for example, are Wi-Fi-enabled smart scales that can track weight, body fat percentage, and Body Mass Index.[59] Each can automatically send you your weight-loss progress.[60] Withings similarly manufactures a blood-pressure cuff that synchronizes with a smartphone.[61] The software application accompanying the device graphs your blood pressure over time and can e-mail results to you or your physician.[62] Similarly, the iBGStar blood glucose monitor connects to an iPhone to track blood sugar levels over time,[63] and Johnson & Johnson's OneTouch Verio sensor can upload such data to an iPhone wirelessly over BlueTooth.[64] Likewise, the Propeller Health sensor-based asthma inhaler tracks the time and place you use your asthma medication and wirelessly sends that information to your smart-phone.[65] The accompanying application allows you to view your sensor data and create an asthma diary.[66]

Countertop devices are a fast growing and rapidly advancing product sector. For example, the Scanadu Scout is a small countertop device that a

---

56. Press Release, Juniper Research, Mobile Healthcare and Medical App Downloads to Reach 44 Million Next Year, Rising to 142 Million in 2016 (Nov. 29, 2011), *available at* http://www.juniperresearch.com/viewpressrelease.php?pr=275, *archived at* http://perma.cc/B92A-WLDP.

57. Ralf-Gordon Jahns, *The Market for mHealth App Services Will Reach $26 Billion by 2017*, RESEARCH2GUIDANCE (Mar. 7, 2013), http://research2guidance.com/the-market-for-mhealth-app-services-will-reach-26-billion-by-2017/, *archived at* http://perma.cc/4ZZJ-E3VX.

58. Michael Yang, *For the Wearable Tech Market to Thrive, It Needs to Get in Better Shape*, GIGAOM (May 4, 2013, 12:00 PM), https://gigaom.com/2013/05/04/for-the-wearable-tech-market-to-thrive-it-needs-to-get-in-better-shape/, *archived at* http://perma.cc/3VJV-KCJJ (citing *Sports and Wellness Drive mHealth Device Shipments to Nearly 30 Million in 2012*, ABIRESEARCH, Dec. 7, 2012, https://www.abiresearch.com/press/sports-and-wellness-drive-mhealth-device-shipments, *archived at* http://perma.cc/6CUE-D3XG).

59. *Fitbit Aria*, FITBIT, http://www.fitbit.com/aria, *archived at* http://perma.cc/9ZVJ-F8SD; *Smart Body Analyzer*, WITHINGS, http://www.withings.com/us/smart-body-analyzer.html, *archived at* http://perma.cc/DA4A-J6D3.

60. *Fitbit Aria*, *supra* note 59; *Smart Body Analyzer*, *supra* note 59.

61. *Wireless Blood Pressure Monitor*, WITHINGS, http://www.withings.com/us/blood-pressure-monitor.html, *archived at* http://perma.cc/874Z-8H65.

62. *Id.*

63. *About iBGStar®*, IBGSTAR®, http://www.ibgstar.us/what-is-ibgstar.aspx, *archived at* http://perma.cc/8P4H-VNAB.

64. *OneTouch® Verio® Sync™*, ONETOUCH®, http://www.onetouch.com/veriosync, *archived at* http://perma.cc/JXC6-PC8Y.

65. *Better Manage Your Asthma and COPD*, PROPELLER HEALTH, http://propellerhealth.com/solutions/patients/, *archived at* http://perma.cc/6AK6-YLG9.

66. *Id.*

user briefly holds up to the forehead to take measurements.[67] It tracks vital signs such as heart rate, body temperature, oximetry (the oxygen in arterial blood), respiratory rate, blood pressure, electrocardiography (ECG), and emotional stress levels.[68] Such comprehensive home measurement was unthinkable even two years ago. Even more dramatic, Scanadu is developing a home urinalysis device—called the Scanadu Scanaflo—that measures "glucose, protein, leukocytes, nitrates, blood, bilirubin, urobilinogen, specific gravity, and pH in urine."[69] It can also test for pregnancy.[70] Again, such analysis is entirely novel for the home consumer market.

Sensor-laden countertop consumer products are becoming more diverse and creative as manufacturers invent new ways to capture data from the objects and environments with which we interact. Podimetrics has developed a sensor-driven floor mat that helps diabetic patients detect foot ulcers.[71] AdhereTech makes an Internet-enabled pill bottle that tracks how many pills remain in a prescription and how often a pill is removed, allowing the company to remind patients to take a pill on schedule.[72] The HAPIfork is a sensor-filled fork that monitors how much and how fast you eat.[73] In addition to uploading its data to a computer or smartphone app, the fork's indicator lights will flash to warn you that you are eating too quickly.[74] Finally, after your meal you can brush with the Beam Brush, which wirelessly connects to a user's smartphone to record the date, time, and duration of "brushing events."[75]

2. Wearable Sensors.—Wearable sensors have also proliferated in the last eighteen months. As indicated, consumers have purchased tens of mil-

67. *Scanadu Scout*™, SCANADU, https://www.scanadu.com/scout/, *archived at* http://perma.cc/LBG6-DZ53.

68. Nathan Hurst, *Scanadu Builds a $149 Personal Tricorder for Non-Trekkies*, WIRED, June 6, 2013, http://www.wired.com/2013/06/scanadu-scout/, *archived at* http://perma.cc/3KVC-D3RN.

69. Press Release, Scanadu, Scanadu Packs More Features Into Scanadu Scout™; Unveils Design For ScanaFlo™ (May 22, 2013), *available at* https://www.scanadu.com/pr/scanadu-packs-more-features-into-scanadu-scout-unveils-design-for-scanaflo/, *archived at* http://perma.cc/ST55-SX6Z.

70. *Id.*

71. Alice Waugh, *Idea Draws on Engineering and Business to Help Diabetics*, MIT NEWS (Jan. 20, 2012), http://newsoffice.mit.edu/2012/podimetrics-lgo-0120, *archived at* http://perma.cc/766-KCWF; *see also* PODIMETRICS, https://www.podimetrics.com/, *archived at* http://perma.cc/UA6R-29SD.

72. *Smart Wireless Pill Bottles*, ADHERETECH, http://www.adheretech.com, *archived at* http://perma.cc/Y3D3-YT4U.

73. *HAPIfork*, HAPI.COM, http://www.hapi.com/product/hapifork, *archived at* http://perma.cc/W3S3-7KBK.

74. *Id.*

75. Eliza Strickland, *Review: Beam Toothbrush*, IEEE SPECTRUM, Jan. 30, 2013, http://spectrum.ieee.org/geek-life/tools-toys/review-beam-toothbrush, *archived at* http://perma.cc/AD62-P5H6.

lions of these devices in the last few years.[76] Many—such as the Fitbit, Nike+ FuelBand, and BodyMedia FIT Armband—are electronic pedometers that track number of steps taken each day, distance walked, and calories burned.[77] Some wearable fitness devices also track other information, such as minutes asleep and quality of sleep,[78] heart rate, perspiration, skin temperature,[79] and even breathing patterns.[80] The FINIS Swimsense tracks what swim stroke you are doing as well as distance swum, speed, and calories burned.[81] Not all inhabit the wrist or arm: Valencell PerformTekfitness devices pack a variety of sensors into a set of earbud headphones,[82] the Pulse is a ring that tracks heart rate,[83] and the Lumo Back posture sensor is a strap worn around the lower back.[84]

Various companies have developed bio-tracking clothing with sensors embedded in the fabric.[85] Such sensor-laden clothing has both fitness and medical applications; some is designed to measure athletic activity. The Electricfoxy Move shirt, for example, contains four embedded stretch-and-bend sensors to monitor movement and provide real-time feedback about yoga poses, Pilates stretches, golf swings, or dance moves.[86] Nike+ sensor-filled shoes can measure running and walking data as well as the height achieved during a basketball dunk.[87] Other products have medical applications. The iTBra, for example, contains integrated sensors in the bra's support cups that monitor slight variations in skin temperature that can provide very early indications of breast cancer.[88] Finally, Sensoria's Fitness

76. *See supra* note 58 and accompanying text.

77. *The Fitbit Philosophy*, FITBIT, http://www.fitbit.com/story, *archived at* http://perma.cc/4ZFW-Y7VE; *Nike+ FuelBand SE*, NIKE, http://www.nike.com/us/en_us/c/nikeplus-fuelband, *archived at* http://perma.cc/ZZJ6-MEYM; *The Science*, BODYMEDIA®, http://www.bodymedia.com/the_science.html, *archived at* http://perma.cc/4PJ-TKJQ.

78. *Fitbit Flex*, FITBIT**,** http://www.fitbit.com/flex, *archived at* http://perma.cc/GBD2-ESFY.

79. *Peak*™, BASIS, https://www.mybasis.com/, *archived at* http://perma.cc/4LKF-XU5X.

80. SPIRE, www.spire.io, *archived at* http://perma.cc/K474-N6YY.

81. *Swimsense® Performance Monitor*, FINIS, http://www.finisinc.com/swimsense.html, *archived at* http://perma.cc/DDJ8-3343.

82. VALENCELL, http://www.performtek.com/, *archived at* http://perma.cc/JKF3-FLQV.

83. *Pulse*, ELECTRICFOXY, http://www.electricfoxy.com/pulse, *archived at* http://perma.cc/626L-F9XT.

84. *Lumo Back*, LUMO, http://www.lumoback.com/lumoback/, *archived at* http://perma.cc/7M6F-SNLC.

85. *E.g.*, AIQ SMART CLOTHING, http://www.aiqsmartclothing.com, *archived at* http://perma.cc/PS2V-BVSX (advertising development of smart-clothing products that integrate technology and textiles); Elizabeth Woyke, *AT&T Plans to Sell Health-Tracking Clothing*, FORBES (Oct. 28, 2011, 2:23 PM), http://www.forbes.com/sites/elizabethwoyke/2011/10/28/att-plans-to-sell-health-tracking-clothing/, *archived at* http://perma.cc/S7V7-HUD5 (describing clothing developed by AT&T that will track "heart rate, body temperature and other vital signs").

86. *Move*, ELECTRICFOXY, http://www.electricfoxy.com/move/, *archived at* http://perma.cc/G4E-6ANP.

87. *Nike+ Basketball*, NIKE, https://secure-nikeplus.nike.com/plus/products/basketball, *archived at* http://perma.cc/TZ9A-2WCK.

88. CYRCADIA HEALTH, http://cyrcadiahealth.com/, *archived at* http://perma.cc/EG6E-MUYA.

smart socks can track not just how far or fast you run, but your running form and technique in order to avoid or diagnose injuries.[89]

Wearable fitness sensors are moving well beyond mere pedometry. The Amiigo wristband, for example, can detect different types of physical activity (e.g., jumping jacks, bicep curls, or jogging) and measure the number of repetitions performed or distances covered.[90] The LIT tracker can measure paddles made in a canoe, jumps made during a basketball game, G-forces incurred during a ski jump, or effort expended surfing.[91] The Atlas tracker can measure heart rate and activity levels for almost any exercise, including swimming (it can distinguish between different strokes); running; weight lifting; pushups; sit-ups; and rock climbing.[92]

3. Intimate Contact Sensors.—Related to wearables but sufficiently distinct to deserve special treatment, intimate contact sensors are devices embedded in bandages, medical tape, patches, or tattoos worn on the skin. Sometimes called "epidermal electronics," these sensors are currently more medical in nature than fitness-oriented. For example, in November 2012, the Food and Drug Administration (FDA) approved the Raiing Wireless Thermometer, a peel-and-stick contact thermometer sensor that transmits real-time body temperature to a user's smartphone.[93] Similarly, MC10's Biostamp is a tiny, flexible prototype device that can be worn like a small Band-Aid.[94] It measures and transmits heart rate, brain activity, body temperature, hydration levels, and exposure to ultraviolet radiation.[95] Sano

89. *Sensoria Fitness Socks*, SENSORIA FITNESS, http://store.sensoriafitness.com/sensoria-fitness-anklet-and-one-pair-of-socks, *archived at* http://perma.cc/NN48-LV9X.

90. *Can Amiigo Track My _____ ?*, AMIIGO, http://updates.amiigo.co/post/84680379473/can-amiigo-track-my, *archived at* http://perma.cc/M8W7-C4YZ.

91. Zach Honig, *NZN Labs Launches Lit, a Social-Enhanced Fitness Tracker for Adventurous Types*, ENGADGET (Apr. 2, 2013, 3:00 PM), http://www.engadget.com/2013/04/02/lit-fitness-tracker/, *archived at* http://perma.cc/759S-9D4N; *see also LIT: An Activity Tracker Ready for Action*, INDIEGOGO, https://www.indiegogo.com/projects/lit-an-activity-tracker-ready-for-action, *archived at* http://perma.cc/ND8D-N38V.

92. ATLAS, http://atlaswearables.com, *archived at* http://perma.cc/3T8E-LTN2; *see also* Brandon Ambrosino, *With Atlas, JHU Alum Poised to Make Big Splash in Wearable Fitness Tracker Market*, HUB, JOHN HOPKINS U. (Jan. 27, 2014), http://hub.jhu.edu/2014/01/27/interview-atlas-peter-li, *archived at* http://perma.cc/7WA8-EVAY (emphasizing that the Atlas can identify and track specific exercises as opposed to general activity).

93. Jonah Comstock, *FDA Clears iPhone-Enabled Body Thermometer*, MOBIHEALTHNEWS (Nov. 16, 2012), http://mobihealthnews.com/19110/fda-clears-iphone-enabled-body-thermometer/, *archived at* http://perma.cc/4NAA-MW2K; *see also iThermonitor*, RAIING, http://www.raiing.com/iThermonitor/, *archived at* http://perma.cc/6E7U-QWRS.

94. Sam Grobart, *MC10's BioStamp: The New Frontier of Medical Diagnostics*, BLOOMBERG BUSINESSWEEK, June 13, 2013, http://www.businessweek.com/articles/2013-06-13/mc10s-biostamp-the-new-frontier-of-medical-diagnostics, *archived at* http://perma.cc/7MHL-ZZDD; *see also Company Overview*, MC10, http://www.mc10inc.com/press-kit/, *archived at* http://perma.cc/A2P9-E6GQ.

95. Grobart, *supra* note 94.

Intelligence is developing a patch to monitor the blood stream.[96] This sensor-filled transdermal patch can record glucose levels, kidney function, potassium levels, and electrolyte balance.[97] The Metria patch by Avery Dennison is a remote medical monitoring device that measures temperature, sleep, heart rate, steps taken, and respiration rates.[98]

4. Ingestible & Implantable Sensors.—Although they may sound overly like science fiction, ingestible and implantable sensors are also becoming a reality. Ingestible sensors include "smart pills," which contain tiny sensors designed to monitor inside the body. Given Imaging, for example, makes the PillCam—a pill-sized camera used to detect bleeding and other problems in the gastrointestinal tract[99]—as well as SmartPill—an ingestible capsule that measures pressure, pH levels, and temperature as it travels through the body.[100] More bizarre, perhaps, in July 2012 the FDA approved the Proteus Feedback System, a pill containing a digestible computer chip.[101] The sensor is powered by the body's stomach fluids and thus needs no battery or antenna.[102] A patch worn on the skin then captures data from the pill to track whether and when the pill was ingested, which it then sends on wirelessly to the user's smartphone.[103] The goal is to embed such sensors into various types of medicines to monitor prescription compliance.

Implantable medical sensors are already being prescribed to monitor blood glucose, blood pressure, and heart function,[104] and newer implantable sensors are being developed to detect organ transplant rejection.[105] One compelling example is a sensor that is implanted in a patient's tooth and that

96. Ariel Schwartz, *No More Needles: A Crazy New Patch Will Constantly Monitor Your Blood*, CO.EXIST, FAST COMPANY (June 19, 2012, 8:00 AM), http://www.fastcoexist.com/1680025/no-more-needles-a-crazy-new-patch-will-constantly-monitor-your-blood, *archived at* http://perma.cc/M7D2-YTY7.

97. *Id.*

98. *Metria™ Informed Health*, AVERY DENNISON, http://www.averydennison.com/en/home/technologies/creative-showcase/metria-wearable-sensor.html, *archived at* http://perma.cc/A5W7-R93J.

99. *PillCam Capsule Endoscopy*, GIVEN IMAGING, http://www.givenimaging.com/en-us/Innovative-Solutions/Capsule-Endoscopy/Pages/default.aspx, *archived at* http://perma.cc/TC97-3NZP.

100. *Motility Monitoring*, GIVEN IMAGING, http://givenimaging.com/en-us/Innovative-Solutions/Motility/SmartPill/Pages/default.aspx, *archived at* http://perma.cc/L8UJ-ZS4M.

101. *Digital Health Feedback System*, PROTEUS DIGITAL HEALTH, http://www.proteus.com/technology/digital-health-feedback-system/, *archived at* http://perma.cc/5UZR-7HGV.

102. *Id.*

103. *Id.*

104. *E.g.*, *Getting an Insertable Cardiac Monitor*, MEDTRONIC, http://www.medtronic.com/patients/fainting/getting-a-device/index.htm, *archived at* http://perma.cc/8REJ-DL5Y (providing medical information on, and testimonials about, subdermal cardiac monitors).

105. *Transplant Rejection Sensor Paves Way for Body-Integrated Electronics*, ENGINEER, July 11, 2013, http://www.theengineer.co.uk/medical-and-healthcare/news/transplant-rejection-sensor-paves-way-for-body-integrated-electronics/1016483.article, *archived at* http://perma.cc/8W3-4W3R.

can differentiate between eating, speaking, coughing, smoking, drinking, and breathing.[106] The device is fitted between two teeth or mounted on dentures or braces and can transmit information wirelessly to one's dentist to assess dental disease or unhealthy habits.[107]

Ingestible and implantable health and fitness sensors are at the cutting edge of current technology, but some estimate that within a decade up to a third of the U.S. population will have either a temporary or permanent implantable device inside their body.[108]

B. Automobile Sensors

Sensors have also become pervasive in the automotive context. Consider three types of automobile sensors that collect enormous amounts of data about drivers: EDRs, consumer automobile sensor products, and auto-insurance telematics devices.

1. Event Data Recorders.—The NHTSA estimates that over 96% of 2013 vehicles—and most cars sold in the United States in the last twenty years—contain EDRs.[109] The NHTSA requires that EDRs collect fifteen types of sensor-based information about a car's condition, including braking status, vehicle speed, accelerator position, engine revolutions per minute, safety-belt usage, air-bag deployment, and number and timing of crash events.[110] The NHTSA requires that EDRs store such information for thirty seconds after a triggering impact, thus providing a composite picture of a car's status during any crash or incident.[111] The NHTSA places no limits on the types of data that can be collected, nor does it specify who owns these data or whether such data can be retained and used by third parties.[112] A manufacturer can thus choose to include additional types of information, such as driver steering input, antilock-brake activity, seat positions for driver and passenger, occupant size or position, vehicle location, phone or radio use, navigation-system use, or other aspects of the car's condition.

2. Consumer Automobile Sensors.—In addition to EDRs, various consumer devices allow a driver to access her car's digital information via a

106. Ross Brooks, *Tooth-Embedded Sensor Relays Eating Habits to the Dentist*, PSFK (July 30, 2013), http://www.psfk.com/2013/07/tooth-sensor-track-eating-habits.html, *archived at* http://perma.cc/EVM4-FV6D.

107. *Id.*

108. Cadie Thompson, *The Future of Medicine Means Part Human, Part Computer*, CNBC (Dec. 24, 2013, 8:00 AM), http://www.cnbc.com/id/101293979, *archived at* http://perma.cc/VQV3-VD82.

109. *See supra* note 22 and accompanying text.

110. 49 C.F.R. §§ 563.6–.7 (2013).

111. *See id.* § 563.11(a).

112. *See id.* (disclosing that some parties, such as law enforcement, may use EDR data, but making no mention regarding who owns EDR data).

smartphone. The leading example is the Automatic Link—a small Bluetooth device that connects to a car's OBD-II port.[113] Described as a "FitBit for your car," the Automatic syncs information to a smartphone to monitor both the car's health and the user's driving habits.[114] The Automatic tracks such variables as whether the driver brakes suddenly, is speeding, or accelerates rapidly—all in the name of helping the driver improve fuel efficiency.[115] It also tracks and records location so as to provide feedback on how much driving you do per week, where, and when.[116] All such information is stored in the cloud on Automatic's servers.[117] The system can be set to automatically call for help in the event of a crash and to e-mail you when your engine needs maintenance.[118]

Much of the same functionality can be had just from the sensors already in a driver's smartphone. Zendrive, for example, is an iPhone application that helps drivers track their driving, providing feedback on driving technique, tips to avoid traffic, and information on nearby attractions.[119] Likewise, DriveScribe is an app designed to help parents and insurers monitor teenage driving habits through the sensor data created by a driver's smartphone.[120] The app can be set to block texting and calling on the teenager's phone while driving, as well as to send an e-mail or text message to a parent with updates on the teenager's driving performance.[121] It records the time, length, and location of every trip; average speed and speed at any point during the trip; and descriptions of any moving violations (e.g., speeding or other detectable infractions, such as failing to obey a stop sign).[122]

These consumer devices differ in important ways from the EDR already in most vehicles. First, an EDR typically can record and store only a few

---

113. AUTOMATIC™, https://www.automatic.com/, *archived at* http://perma.cc/4NMD-6NZR.

114. Jamie Todd Rubin, *Testing Automatic Link, the FitBit for Your Car*, DAILY BEAST (July 8, 2014), http://www.thedailybeast.com/articles/2014/07/08/testing-automatic-link-the-fitbit-for-your-car.html, *archived at* http://perma.cc/KRN7-AEVX.

115. AUTOMATIC™, *supra* note 113.

116. *Id.*

117. *Legal Information*, AUTOMATIC™, https://www.automatic.com/legal/, *archived at* http://perma.cc/324H-FFG3.

118. AUTOMATIC™, *supra* note 113. The Dash is a similar device. DASH, http://dash.by, *archived at* http://perma.cc/4F43-CN2E. Similarly, the Mojio is a prototype Internet-connected car monitoring sensor that can alert a user if their car has been damaged, stolen, towed, or needs service. MOJIO, http://www.moj.io, *archived at* http://perma.cc/S7FG-68B4.

119. *Zendrive Seed Funding*, ZENDRIVE BLOG (Aug. 29, 2013), http://zendriveblog.tumblr.com/post/59408227794/zendrive-seed-funding-08-29-13-at-facebook-and, *archived at* http://perma.cc/5MHH-TX2Q; *see also* ZENDRIVE, http://www.zendrive.com, *archived at* http://perma.cc/XR63-ZYN3.

120. DRIVESCRIBE, http://www.drivescribe.com, *archived at* http://perma.cc/6NMV-F4CM.

121. *Keeping Teens Safe*, DRIVESCRIBE, http://drivescribe.com/parents, *archived at* http://perma.cc/VC5C-MKLC.

122. *Driver Performance*, DRIVESCRIBE, http://drivescribe.com/driver-performance/, *archived at* http://perma.cc/3AFU-FK26.

seconds of data—enough to assist with crash diagnostics, but not enough to track a vehicle's location or a driver's performance over time. Consumer smartphone-connected (or smartphone-based) apps record much more information and store it longitudinally. Second, an EDR stores its limited information in the car on the device itself. Consumer driving monitors and smartphone apps transmit such information to the device's manufacturer and often store such information in the cloud. Third, obviously the notice involved to consumers differs. Many consumers may be unaware that their vehicle contains an EDR, which may be mentioned only in the owner's manual.[123] Presumably consumers are aware, however, when they install a consumer sensor device in their car or a car-tracking app on their smartphone.

3. Auto-Insurance Telematics Devices.—Finally, a third type of automobile sensor device has become increasingly popular: insurance telematics devices. These products are given to consumers by automobile insurers to track consumer driving behavior and offer discounts on insurance premiums based on driving behavior.[124]

The most well-known telematics device in the United States is probably the Progressive Snapshot.[125] Progressive provides the Snapshot device to insureds, who connect it to their vehicles. The Snapshot device collects information on vehicle speed, time of day, miles driven, and frequency of hard braking.[126] It does not collect information on driver identity.[127] After thirty days of data collection, the data are used to calculate a "Snapshot score" for that vehicle (or driver), which is then used as one factor in determining the applicable insurance premium.[128] Snapshot then continues to collect data for another five months to set the ongoing renewal discount for that policy.[129]

123. 49 C.F.R. § 563.11(a) (2013).

124. Bill Kenealy, *Wireless Sensors Provide Underwriters with Expanded Data*, BUS. INS. (Jan. 13, 2013, 6:00 AM), http://www.businessinsurance.com/article/20130113/NEWS04/301139980, *archived at* http://perma.cc/7ES8-TB2Y (emphasizing that insurance telematics devices allow automobile insurers to tailor rates to individual policyholders based on their individual behavior rather than generalized assumptions). These categories have begun to blur. In September 2014, Progressive announced a partnership with Zubie, the manufacturer of a consumer automobile tracking device, whereby Zubie customers will be able to see how Progressive would insure them based on data Zubie has collected. Stacey Higginbothham, *Connected Car Company Zubie Signs Deal with Progressive*, GIGAOM (Sept. 4, 2014, 6:30 AM), https://gigaom.com/2014/09/04/connected-car-company-zubie-signs-deal-with-progressive/, *archived at* http://perma.cc/5RWV-PLSR.

125. *Snapshot®*, PROGRESSIVE, http://www.progressive.com/auto/snapshot/, *archived at* http://perma.cc/U6PP-H5YV.

126. *Terms & Conditions for Snapshot®*, PROGRESSIVE, http://www.progressive.com/auto/snapshot-terms-conditions/, *archived at* http://perma.cc/V2ZV-ZWA6.

127. *See id.*

128. *Id.*

129. *Snapshot® Common Questions*, PROGRESSIVE, http://www.progressive.com/auto/snapshot-common-questions/, *archived at* http://perma.cc/C9JN-5NH3.

According to Progressive's privacy policy, Snapshot data are not used to resolve insurance claims without the user's consent.[130]

Snapshot and other usage-based devices have grown in popularity, but enrollment remains low as a percentage of the total insurance industry. Overall, roughly three percent of insureds use a telematics device, although roughly ten percent of Progressive's customer portfolio uses Snapshot.[131] Insurance executives continue to look for marketing approaches to reassure consumers about privacy concerns.[132] Some have expressed concern that manufacturers of consumer automobile telematics systems may not be disclosing sufficient information about the data collected or the ways such data are used.[133] However, industry generally minimizes concerns about privacy, equity, and discrimination. Instead, industry commentators tout the benefits of more accurate pricing[134]—and even of the changes that individuals might make to their behavior because of increased monitoring.[135] Insurance-industry commentators speculate that the telematics revolution may spread from car insurance to health and life insurance.[136]

130. *Snapshot® Privacy Statement*, PROGRESSIVE, http://www.progressive.com/auto/snapshot-privacy-statement/, *archived at* http://perma.cc/K7ZM-2SRN.

131. Becky Yerak, *Motorists Tap the Brakes on Installing Data Devices for Insurance Companies*, CHI. TRIB., Sept. 15, 2013, http://articles.chicagotribune.com/2013-09-15/classified/ct-biz-0915—telematics-insure-20130915_1_insurance-companies-insurance-telematics-progressive-snapshot, *archived at* http://perma.cc/72WC-SS64.

132. *See id.* (stressing that actual adoption of automobile telematics devices is contingent on educating consumers about the boundaries and limits of data collection and disclosure).

133. *See generally* Francesca Svarcas, *Turning a New Leaf: A Privacy Analysis of Carwings Electric Vehicle Data Collection and Transmission*, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 165 (2012) (scrutinizing Nissan's privacy practices regarding the telematics systems in Nissan LEAF vehicles).

134. *See, e.g.*, Lilia Filipova-Neumann & Peter Welzel, *Reducing Asymmetric Information in Insurance Markets: Cars with Black Boxes*, 27 TELEMATICS & INFORMATICS 394, 402 (2010) (concluding that the use of black box data to obtain "perfect information" on individual drivers would alleviate informational asymmetry and, with some restrictions, could result in a Pareto improvement of overall welfare); Yuanshan Lee, *Applications of Sensing Technologies for the Insurance Industry*, *in* BUSINESS ASPECTS OF THE INTERNET OF THINGS 8, 8–9 (Florian Michahelles ed., 2008) (analyzing how the implementation of sensor-based technology could result in more accurate and personalized pay-as-you-drive premiums based on actual mileage rather than generalized mileage proxies).

135. *See* Anthony O'Donnell, *Will Data Proliferation Foster Insurer/Customer Collaboration on Underwriting?*, INS. & TECH., INFORMATIONWEEK (Nov. 19, 2010, 9:17 AM), http://www.insurancetech.com/business-intelligence/228300215, *archived at* http://perma.cc/9CVH-2UVG ("This new kind of data-driven transactional environment could also provide the incentive for individuals to act more virtuously.").

136. *See id.* ("Perhaps life and health insurance customers may similarly be motivated to enter into a kind of information transparency partnership whereby they enjoy better rates for demonstrating less risky behavior.").

C. Home & Electricity Sensors

Internet of Things devices have entered the home as well. Consider two applications: the "smart home" of connected Internet of Things devices and the "smart grid" of sensor-based electricity monitors.

1. The Smart Home.—The phrase "Internet of Things" often conjures up images of a home full of connected, sensor-laden devices. As discussed above, sensor devices go far beyond such smart home appliances. Nevertheless, such home electronics are indeed one aspect of the proliferation of sensors.

There are many new consumer sensor devices available for home use. The most well-known may be the Nest thermostat. The Nest thermostat—recently acquired by Google in the first major Internet of Things acquisition[137]—tracks your behavior at home to set temperature more efficiently.[138] The thermostat accepts and records direct user input (e.g., to increase or decrease temperature) but also contains sensors to sense motion in a room, ambient light, room temperature, and humidity.[139] All such information is stored on Nest's cloud servers and can be accessed and controlled via a user's smartphone or other Internet-connected computer.[140] Nest also makes a smoke and carbon monoxide detector with similar features.[141]

Beyond thermostats and smoke detectors, a variety of home appliances are increasingly Internet connected. The GE Brillion home oven, for example, reports its temperature, sends alerts, and can be turned on or controlled from a GE smartphone app.[142] More broadly, the DropTag sensor can detect if a package has been dropped or shaken during shipping;[143] a Twine sensor device can detect floods, leaks, opened doors, temperature, and other events

137. Rolfe Winkler & Daisuke Wakabayashi, *Google to Buy Nest Labs for $3.2 Billion*, WALL ST. J., Jan. 13, 2014, http://online.wsj.com/news/articles/SB10001424052702303595404579318952802236612, *archived at* http://perma.cc/5T7W-2DNG.

138. *Life with Nest Thermostat*, NEST, https://nest.com/thermostat/life-with-nest-thermostat/, *archived at* http://perma.cc/L94A-Y63V.

139. *Explore Your Nest*, NEST, https://nest.com/thermostat/inside-and-out/#explore-your-nest, *archived at* http://perma.cc/QTX5-RRNM.

140. *What Does Nest Do with Private Data?*, NEST, http://support.nest.com/article/What-does-Nest-do-with-private-data, *archived at* http://perma.cc/K58S-RKVF.

141. *Life With Nest Protect*, NEST, https://nest.com/smoke-co-alarm/life-with-nest-protect/, *archived at* http://perma.cc/5A8Y-MTFR.

142. *GE Brillion™ Connected Home FAQs*, GE APPLIANCES, http://www.geappliances.com/connected-home-smart-appliances/brillion-appliances-faqs.htm, *archived at* http://perma.cc/DN5S-UPTN.

143. Press Release, Cambridge Consultants, Delivering Peace of Mind (Feb. 6, 2013), *available at* http://www.cambridgeconsultants.com/news/pr/release/116/en, *archived at* http://perma.cc/Q3P3-D7SB.

in your home;[144] a Wattvision will record home energy-use patterns;[145] and a Wimoto Growmote will text you if your plants need watering.[146] Various firms are working to integrate such disparate sources of information onto software and hardware platforms. SmartThings, for example, consists of a processing hub that can connect to a variety of different home sensors, such as an open/shut sensor (to monitor doors and windows); a vibration sensor (to monitor knocking on the front door); a temperature sensor (to control a thermostat); a motion sensor; and a power-outlet monitor (to turn outlets on and off remotely).[147] Similarly, Belkin is developing a network of home devices to monitor home electricity and water usage and to allow consumer control over power outlets and home devices;[148] Sense has created the Mother line of motion and other sensors to track many aspects of daily life, including sleep, fitness, medication compliance, water usage, home temperature, and home security;[149] Revolv is a smart home hub designed to work with multiple brands of connected appliances;[150] and Quirky markets a line of smart home products designed by GE and other manufacturers to work together.[151] All of these consumer products aim to provide users with information about and control over home appliances. Along the way, they generate, transmit, and store a great deal of information about both a home and those within it.

2. The Smart Grid.—The home is increasingly monitored via sensors in a second way as well: the smart electricity grid. According to the U.S. Energy Information Administration, more than 36 million smart electricity meters were installed in the United States as of August 2012, covering roughly 25%

144. *Twine*, SUPERMECHANICAL, http://www.supermechanical.com/twine/, *archived at* http://perma.cc/CVX8-S8MR.

145. *How It Works*, WATTVISION, http://www.wattvision.com/info/how_it_works, *archived at* http://perma.cc/3DY2-RYWV.

146. WIMOTO, http://www.wimoto.com, *archived at* http://perma.cc/YLY8-XWVT.

147. *SmartThings Hub*, SMARTTHINGS, https://shop.smartthings.com/#!/products/smartthings-hub, *archived at* http://perma.cc/323Z-SXHX; *see Things Shop*, SMARTTHINGS, https://shop.smartthings.com/#!/products, *archived at* http://perma.cc/U5RM-DQYC (listing various sensors and devices that may be connected to the SmartThings Hub and controlled by the app).

148. Press Release, HydroPoint Data Sys., Inc., HydroPoint Partners with Belkin to Introduce 360º Smart Water Management (Apr. 30, 2013), *available at* http://www.hydropoint.com/hydropoint-partners-with-belkin-to-introduce-360-smart-water-management/, *archived at* http://perma.cc/TV3R-WAPY.

149. *Mother*, SEN.SE, https://sen.se/store/mother/, *archived at* http://perma.cc/6EJ6-UVFQ.

150. REVOLV, http://revolv.com, *archived at* http://perma.cc/GNA2-WNLA.

151. *Quirky + GE*, QUIRKY, https://www.quirky.com/shop/quirky-ge, *archived at* http://perma.cc/UW78-DUR3; *see* Steve Lohr, *Quirky to Create a Smart-Home Products Company*, N.Y. TIMES, June 22, 2014, http://www.nytimes.com/2014/06/23/technology/quirky-hopes-wink-will-speed-adoption-of-smart-home-products.html?_r=0, *archived at* http://perma.cc/5FZV-5HSC (detailing how Quirky has partnered with General Electric and other manufacturing firms to help ease these companies' entry into the smart home market).

of the U.S. electric market.[152] The smart grid such meters create promises huge energy efficiencies.[153]

At the same time, smart grid data provide an intimate look into one's home. Electricity usage can reveal when a person is or is not home; how often they cook, clean, shower, or watch television; how often they go on vacation; and how often they use exercise equipment. Computer-science research has even shown that one can determine—with 96% accuracy—exactly what program or movie someone is watching on television just by monitoring electrical signals emanating from the person's house.[154]

One can infer a great deal from such data, such as how affluent a person is, how diligent a person is about cleanliness or exercise, and even how depressed or sleep-deprived a person may be:

> For example: the homeowner tends to arrive home shortly after the bars close; the individual is a restless sleeper and is sleep deprived; the occupant leaves late for work; the homeowner often leaves appliances on while at work; the occupant rarely washes his/her clothes; the person leaves their children home alone; the occupant exercises infrequently.[155]

As with other forms of sensor data, such information could be of interest to insurance companies, employers, creditors, and law enforcement.[156] And it is very hard to opt out of the smart grid, because utility companies roll smart meters out to an entire geographic area.[157]

The European Data Protection Supervisor has warned that such monitors could lead to "massive collection of personal data" without much protection.[158] Similarly, the National Institute of Standards and Technology recently warned that:

---

152. *Smart Meter Deployments Continue to Rise*, TODAY IN ENERGY, U.S. ENERGY INFO. ADMIN. (Nov. 1, 2012), http://www.eia.gov/todayinenergy/detail.cfm?id=8590, *archived at* http://perma.cc/A87C-3MXN.

153. *See id.* (explaining how smart meters can provide real time prices to customers based on time-of-day options so that customers can shift their energy use to a time of day when demand and prices are lower).

154. *See* Miro Enev et al., *Televisions, Video Privacy, and Powerline Electromagnetic Interference*, *in* CCS'11: PROCEEDINGS OF THE 18TH ACM CONFERENCE ON COMPUTER & COMMUNICATIONS SECURITY 537, 538 (2011) (explaining how the authors matched fifteen-minute electromagnetic intereference measurements to a database of "1200 movie minutes 96% of the time").

155. Ann Cavoukian et al., *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, 3 IDENTITY INFO. SOC'Y 275, 284 (2010).

156. CYBER SECURITY WORKING GRP., NAT'L INST. OF STANDARDS AND TECH., NISTIR 7628, GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 28 (Aug. 2010) [hereinafter PRIVACY AND THE SMART GRID].

157. *See* Balough, *supra* note 47, at 175 (explaining that utilities may cease servicing traditional meters altogether as new smart meters are issued across a utility provider's area of service).

158. *Executive Summary of the Opinion of the European Data Protection Supervisor on the Commission Recommendation on Preparations for the Roll-Out of Smart Metering Systems*, 2012 O.J. (C 335) 13, 14, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CEL

> Personal energy consumption data . . . may reveal lifestyle information that could be of value to many entities, including vendors of a wide range of products and services. Vendors may purchase attribute lists for targeted sales and marketing campaigns that may not be welcomed . . . . Such profiling could extend to . . . employment selection, rental applications, and other situations that may not be welcomed by those targets.[159]

Nevertheless, only a few states have addressed how smart grid data can be used, how it should be secured, and what sorts of consent consumers should be required to provide for its use.[160] The California Public Utilities Commission and the National Institute of Standards and Technology collaborated on a report detailing the potential privacy problems with smart grid technology.[161] One state has required utility companies to secure a homeowner's express consent before installing a smart grid device,[162] and five states have enacted legislation allowing consumers to opt out of using smart grid technology.[163] Several states have also limited a utility company's ability to sell or share smart grid data with third parties.[164] To date, however, such regulation of the smart grid is inconsistent and scattered.

D. Employee Sensors

Beyond the body, car, or home, sensors are also being deployed in the workplace, allowing new forms of employee monitoring and control. As in other contexts, workplace sensors create new streams of data about where employees are during the workday, what they are doing, how long their tasks take, and whether they comply with employment rules.

Consider a simple example. HyGreen is a hand-hygiene monitoring system to record all hand-hygiene events in a hospital and remind health-care workers to wash their hands.[165] The system consists of sink-top sensors that

---

EX:52012XX1101(06)&qid=1413041613906&from=EN, *archived at* http://perma.cc/M8QG-86N8.

159. PRIVACY AND THE SMART GRID, *supra* note 156, at 28.

160. *See id.* at 10 (reporting that most state utility commissions have not promulgated privacy policies regarding smart grid data collection).

161. *Id.* at 35–37.

162. N.H. REV. STAT. ANN. § 374:62(II)(a) (Supp. 2013).

163. *Id.* § 374:62(III); VT. STAT. ANN. tit. 30, § 2811(b)(2)–(3) (Supp. 2013); H.R. 4315, 97th Leg., Reg. Sess. (Mich. 2013); H.R. 5027, 2013 Gen. Assemb., Reg. Sess. (R.I. 2013); S. 7184, 235th Leg., Reg. Sess. (N.Y. 2012).

164. *See, e.g.*, CAL. PUB. UTIL. CODE § 8380(b), (e) (West 2013) (prohibiting utility companies from sharing a customer's electric or gas consumption to a third party unless the identifying information is removed or the customer consents); OKLA. STAT. ANN. tit. 17, §§ 710.4, 710.7 (West Supp. 2014) (prescribing standards to govern the access to and use of usage data from smart grid and smart meter technologies); H.R. 11-1191, 68th Gen. Assemb., 1st Reg. Sess. (Colo. 2011) (prohibiting clearinghouses from selling or providing customer consumer data or personally identifiable information without consent).

165. *Hand Hygiene Recording and Reminding System*, HYGREEN®, http://www.hygreen.com/, *archived at* http://perma.cc/5WK8-AZYM.

detect soap dispensing and hand washing. When a hand-hygiene event is recognized, the sensors read the employee's identification badge and wirelessly transmit a record of the employee's identity and the time and location of the hand-washing event.[166] If the employee has not washed her hands and approaches a patient's bed, another sensor on the bed registers that the employee is approaching and sends the employee's identification badge a warning signal, causing the badge to vibrate to remind the employee to wash.[167] The system tracks and stores all hand washing by employees around the clock.[168]

This is a direct and fairly obvious use of sensors to monitor employees and shape their behavior. Location and movement tracking is another relatively simple use. As one commentator recently noted:

> As Big Data becomes a fixture of office life, companies are turning to tracking devices to gather real-time information on how teams of employees work and interact. Sensors, worn on lanyards or placed on office furniture, record how often staffers get up from their desks, consult other teams and hold meetings.[169]

The Bank of America, for example, has used sensor badges to record call-center employees' movements and tone of voice throughout the day.[170]

Other examples of such relatively simple sensor systems include fleet tracking of company trucks or automobiles. For example, Cloud Your Car makes a small device that plugs into a car's cigarette lighter and contains a GPS tracker, cell connectivity, and a variety of accelerometer sensors.[171] It is designed to help business owners track their fleet of vehicles, as well as monitor employee driving behavior.[172] An employer can, for example, monitor fleet status and locations in real time, review route histories, and track employees' driving rankings and scores.[173] Similarly, GreenRoad

---

166. *HyGreen and Hand Hygiene: How It Works*, HYGREEN®, http://www.hygreen.com/HandHygieneMonitor/How.asp, *archived at* http://perma.cc/HU5B-5W9L.

167. *Id.*

168. Other hand-washing systems exist as well. *See, e.g.*, *MedSense*™, GENERAL SENSING, http://www.generalsensing.com, *archived at* http://perma.cc/4Y6H-ALRF (providing a hand-hygiene compliance and monitoring system similar to the HyGreen); *See What i^{M} Is All About*, INTELLIGENT^{M}, http://www.intelligentm.com, *archived at* http://perma.cc/FYQ4-T2FJ (offering a wristband providing similar functions to the MedSense and HyGreen). *See generally* Anemona Hartocollis, *With Money at Risk, Hospitals Push Staff to Wash Hands*, N.Y. TIMES, May 28, 2013, http://www.nytimes.com/2013/05/29/nyregion/hospitals-struggle-to-get-workers-to-wash-their-hands.html, *archived at* http://perma.cc/YL3Y-ZJ5S (chronicling the efforts of hospitals to improve hygiene compliance through the use of technology).

169. Rachel Emma Silverman, *Tracking Sensors Invade the Workplace*, WALL ST. J., Mar. 7, 2013, http://online.wsj.com/news/articles/SB10001424127887324034804578344303429080678, *archived at* http://perma.cc/9X3V-PMKR.

170. *Id.*

171. *Fleet Management for Small Businesses*, CLOUD YOUR CAR, https://www.cloudyourcar.com/product/?lang=None, *archived at* http://perma.cc/A5EB-JFHU.

172. *Id.*

173. *Id.*

manufactures fleet-tracking sensors designed to reduce accident, fuel, insurance, and maintenance costs by providing real-time driving and location information to employers.[174]

Sensors are being used to track more nuanced and abstract aspects of employee behavior as well. For example, Sociometric Solutions has deployed tracking devices for Bank of America, Steelcase, and Cubist Pharmaceuticals.[175] Employees wear a sensor-laden identification badge that contains a microphone, a Bluetooth transmitter, a motion sensor, and an infrared beam.[176] The microphone is not used to record the content of conversations, but instead to assess the tone of voice being used.[177] The higher the pitch or the faster the speech, the more excited or passionate the speaker.[178] Similarly, the infrared beam is used to determine how one user is positioned vis-à-vis another wearing a similar badge.[179] Those who generally have others facing them when speaking are inferred to be more dominant personalities.[180]

Such sensors allow for some amazing inferences. Combined with e-mail traffic data and survey results, one company found that more socially engaged employees performed better, as opposed to employees that spent more time alone in their offices.[181] As a result, the employer set a daily afternoon coffee break—to encourage social interaction.[182] This relatively benign example may not cause alarm. Such data, however, are extremely telling: the CEO of Sociometric Solutions says that he can "divine from a worker's patterns of movement whether that employee is likely to leave the company, or score a promotion."[183] As MIT Professor Alex Pentland put it: "[w]e've been able to foretell, for example, which teams will win a business plan contest, solely on the basis of data collected from team members wearing badges at a cocktail reception."[184]

---

174. *GreenRoad Features*, GREENROAD™, http://greenroad.com/tour/features/, *archived at* http://perma.cc/US4Q-ECRP.

175. Vivian Giang, *Companies Are Putting Sensors on Employees to Track Their Every Move*, BUS. INSIDER (Mar. 14, 2013, 6:23 PM), http://www.businessinsider.com/tracking-employees-with-productivity-sensors-2013-3, *archived at* http://perma.cc/A9BM-AM8V.

176. *Id.* Hitachi has also developed a similar employee ID badge, the Hitachi Business Microscope, containing various sensors for nuanced monitoring of employee interactions and productivity. H. James Wilson, *Wearable Gadgets Transform How Companies Do Business*, WALL ST. J., Oct. 20, 2013, http://online.wsj.com/news/articles/SB10001424052702303796404579099203059125112, *archived at* http://perma.cc/X337-N3H9.

177. Giang, *supra* note 175.

178. *Id.*

179. *Id.*

180. *Id.*

181. *See* Alex "Sandy" Pentland, *The New Science of Building Great Teams*, HARV. BUS. REV., Apr. 2012, at 60, 62 (concluding that communication patterns are "the most important predictor of a team's success").

182. *Id.*

183. Silverman, *supra* note 169.

184. Pentland, *supra* note 181, at 63.

There has been relatively little discussion in the legal or business literatures about such sensor-based employee monitoring.[185] Some fear that consent in the employment context is difficult to assess and rarely truly consensual.[186] This potentially becomes more problematic as employers demand access to more intimate information about their employees. The British grocery store chain Tesco, for example, has required employees to wear armbands that measure their productivity.[187] These Motorola devices track how quickly employees unload and scan goods in Tesco's warehouse, as well as how often employees take breaks.[188]

E. Smartphone Sensors

Finally, the most ubiquitous new sensor technologies are those embedded in smartphones. Such phones now generally contain a compass (to detect physical orientation); accelerometer (to track the phone's movement in space); ambient light monitor (to adjust screen brightness); proximity sensor (to detect whether the phone is near your face); and gyroscope (to detect the phone's orientation vertically or horizontally), as well as GPS, a sensitive microphone, and multiple cameras.[189] Research is underway to further enhance smartphones to detect ultraviolet radiation levels (to help prevent skin cancer);[190] pollution levels (to help monitor one's

185. *See, e.g.*, Mika, *supra* note 47, at 2 ("[A]n employer can monitor virtually everything and almost anything can be done with it."); Paul M. Secunda, *Privatizing Workplace Privacy*, 88 NOTRE DAME L. REV. 277, 281–82 (2012) (arguing that public-sector employees should enjoy greater privacy rights than private-sector employees).

186. *See, e.g.*, Adam D. Moore, *Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy*, 10 BUS. ETHICS Q. 697, 701–02 (2000) (discussing how circumstances, such as job scarcity and high unemployment, create an environment wherein employees agree to employer monitoring more out of fear of adverse consequences than actual consent).

187. Claire Suddath, *Tesco Monitors Employees with Motorola Armbands*, BLOOMBERG BUSINESSWEEK, Feb. 13, 2013, http://www.businessweek.com/articles/2013-02-13/tesco-monitors-employees-with-motorola-arm-bands, *archived at* http://perma.cc/6J4K-697V.

188. *Id.*

189. David Nield, *Making Sense of Sensors: What You Don't Know Your Phone Knows About You*, TECHRADAR (Apr. 30, 2014), http://www.techradar.com/us/news/phone-and-communications/mobile-phones/sensory-overload-how-your-smartphone-is-becoming-part-of-you-1210244/1, *archived at* http://perma.cc/Z6EF-DGX7.

190. *See* Thomas Fahrni et al., *Sundroid: Solar Radiation Awareness with Smartphones*, *in* UBICOMP'11: PROCEEDINGS OF THE 2011 ACM CONFERENCE ON UBIQUITOUS COMPUTING 365, 367–70 (2011) (designing a "wearable system to measure solar radiation" using a smartphone and external sensor).

environment);[191] and various indicators of health, activity, and well-being,[192] including sensors that can monitor blood alcohol levels and body fat.[193]

A great deal of information can be gleaned from a typical smartphone. For example, the RunKeeper and Strava applications use an iPhone's sensors and GPS to track running and cycling routes, speeds, and history.[194] The Instant Heart Rate app uses a smartphone's camera to detect a user's fingertip pulse.[195] The Argus and Moves apps track a user's fitness by using a phone's sensors to monitor steps taken, cycling distances, and calories expended, just like a dedicated fitness monitor such as Fitbit.[196]

More personal, perhaps, researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood;[197] stress levels;[198] personality type;[199] bipolar disorder;[200] demographics (e.g., gender, marital

191. *See* DAVID HASENFRATZ ET AL., PARTICIPATORY AIR POLLUTION MONITORING USING SMARTPHONES (2012), *available at* http://research.microsoft.com/en-us/um/beijing/events/ms_ipsn12/papers/msipsn-hasenfratz.pdf, *archived at* http://perma.cc/JL22-Q7VM (designing a measurement system for participatory air-quality monitoring using a smartphone and external sensor).

192. *See* Sean T. Doherty & Paul Oh, *A Multi-Sensor Monitoring System of Human Physiology and Daily Activities*, 18 TELEMEDICINE AND E-HEALTH 185, 185 (2012) (combining smartphone GPS sensors with other physiological sensors to study "the effects of human geographies . . . on human physiology at a very fine spatial/temporal scale").

193. Andrew Ku, *Smartphones Spotted with Breathalyzer, Body Fat Sensors*, TOM'S HARDWARE (Mar. 2, 2012, 3:00 AM), http://www.tomshardware.com/news/NTTidocomo-smartphone-breathalyzer-weather-health,14863.html, *archived at* http://perma.cc/L63Q-QGW6.

194. *Features*, STRAVA, http://www.strava.com/features, *archived at* http://perma.cc/3P82-G3JM; RUNKEEPER, http://www.runkeeper.com, *archived at* http://perma.cc/48RD-7QSA.

195. *Instant Heart Rate*, AZUMIO, http://www.azumio.com/apps/heart-rate/, *archived at* http://perma.cc/DM6R-4WS3.

196. Roy Furchgott, *The Argus App Can Help to Keep You Fit*, N.Y. TIMES, July 23, 2013, http://www.nytimes.com/2013/07/25/technology/personaltech/the-argus-app-can-help-to-keep-you-fit.html?_r=0, *archived at* http://perma.cc/Q2DM-5FLY; MOVES, http://www.moves-app.com/, *archived at* http://perma.cc/7SXX-ZBVF.

197. Robert LiKamWa et al., *MoodScope: Building a Mood Sensor from Smartphone Usage Patterns*, *in* MOBISYS'13: PROCEEDINGS OF THE 11TH ANNUAL INTERNATIONAL CONFERENCE ON MOBILE SYSTEMS, APPLICATIONS, AND SERVICES 389, 400 (2013); *see also* ROBERT LIKAMWA ET AL., CAN YOUR SMARTPHONE INFER YOUR MOOD? 1 (2011), http://research.microsoft.com/en-us/um/redmond/events/phonesense2011/papers/MoodSense.pdf, *archived at* http://perma.cc/7K2E-Q36T (concluding that smartphone usage patterns reliably can be used to infer a user's mood).

198. *See* Amir Muaremi et al., *Towards Measuring Stress with Smartphones and Wearable Devices During Workday and Sleep*, 3 BIONANOSCIENCE 172, 174–78 (2013) (describing a process to infer a user's stress level using data collected from a wearable sensor, the smartphone's internal sensors, and a person's usage of the smartphone).

199. *See* Gokul Chittaranjan et al., *Who's Who with Big-Five: Analyzing and Classifying Personality Traits with Smartphones*, *in* ISWC 2011: 15TH ANNUAL INTERNATIONAL SYMPOSIUM ON WEARABLE COMPUTERS 29, 30 (2011) ("The personality of a user might also determine the kind of functionality that the individual is disposed to use on the phone.").

200. Agnes Grünerbl et al., *Towards Smart Phone Based Monitoring of Bipolar Disorder*, *in* MHEALTHSYS 2012: PROCEEDINGS OF THE SECOND ACM WORKSHOP ON MOBILE SYSTEMS, APPLICATIONS, AND SERVICES FOR HEALTHCARE, at art. 3 (2012).

status, job status, age);[201] smoking habits;[202] overall well-being;[203] progression of Parkinson's disease;[204] sleep patterns;[205] happiness;[206] levels of exercise;[207] and types of physical activity or movement.[208] As evidence mounts of the many different inferences that smartphone sensors can support, researchers are beginning to imagine future phones that will be able to couple such sensor data with other information to understand even more about a user. One computer scientist has predicted that such next-generation devices will be "cognitive phones."[209] Such a phone might be able to combine sensor-based indications of stress, for example, with information from one's calendar about what meeting or appointment caused the stress, information from other sensors about one's health, and location information about where you were at the time the stress occurred. Imagine that "the phone's calendar overlays a simple color code representing your stress levels so you can visually understand at a glance what events, people, and places in the past—and thus likely in the future—aren't good for your mental health."[210] As

201. *E.g.*, Erheng Zhong et al., *User Demographics Prediction Based on Mobile Data*, 9 PERVASIVE & MOBILE COMPUTING 823, 823–24 (2013) (discussing how demographic information may be predicted based on usage and sensor data gleaned from the user's smartphone).

202. *See* F. Joseph McClernon & Romit Roy Choudhury, *I Am Your Smartphone, and I Know You Are About to Smoke: The Application of Mobile Sensing and Computing Approaches to Smoking Research and Treatment*, 15 NICOTINE & TOBACCO RES. 1651, 1652 (2013) ("[M]any of the conditions antecedent to smoking exhibit a 'fingerprint' on multiple sensing dimensions, and hence can be detected by smartphones.").

203. *See* Nicholas D. Lane et al., *BeWell: Sensing Sleep, Physical Activities and Social Interactions to Promote Wellbeing*, 19 MOBILE NETWORKS & APPLICATIONS 345, 347–49 (2014) (describing how the BeWell+ app monitors everyday activity and calculates a user's "wellbeing scores" based on data gathered from the smartphone's sensors).

204. *See* Sinziana Mazilu et al., *Online Detection of Freezing of Gait with Smartphones and Machine Learning Techniques*, *in* 2012 6TH INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING TECHNOLOGIES FOR HEALTHCARE AND WORKSHOPS 123, 123–24 (2012) (proposing the use of smartphones' internal sensors to correct, alert, and treat a user's freezing of gait caused by Parkinson's Disease).

205. Zhenyu Chen et al., *Unobtrusive Sleep Monitoring Using Smartphones*, *in* 2013 7TH INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING TECHNOLOGIES FOR HEALTHCARE AND WORKSHOPS 145, 145 (2013).

206. *See* Andrey Bogomolov et al., *Happiness Recognition from Mobile Phone Data*, *in* SOCIALCOM 2013: ASE/IEEE INTERNATIONAL CONFERENCE ON SOCIAL COMPUTING 790, 790 (2013) (proposing the use of smartphone usage patterns, such as social interactions, to measure happiness rather than self-reported surveys).

207. *See* Muhammad Shoaib et al., *Towards Physical Activity Recognition Using Smartphone Sensors*, *in* UIC-ATC 2013: PROCEEDINGS OF 2013 IEEE 10TH INTERNATIONAL CONFERENCE ON UBIQUITOUS INTELLIGENCE & COMPUTING AND 2013 IEEE 10TH INTERNATIONAL CONFERENCE ON AUTONOMIC & TRUSTED COMPUTING 80, 80 (2013) (analyzing how a smartphone's accelerometer, gyroscope, and magnetometer can be used to collect data about a user's physical activities).

208. Alvina Anjum & Muhammad U. Ilyas, *Activity Recognition Using Smartphone Sensors*, *in* 2013 IEEE CONSUMER COMMUNICATIONS AND NETWORKING CONFERENCE (CCNC) 914, 918–19 (2013).

209. Andew Campbell & Tanzeem Choudhury, *From Smart to Cognitive Phones*, IEEE PERVASIVE COMPUTING, July–Sept. 2012, at 7, 11.

210. *Id.*

futuristic as this may sound, such devices are actually possible by combining different aspects of today's technology.

II. Four Problems

Part I provided a taxonomy of types of consumer devices—personal health monitors, automobile black boxes, home and appliance monitors, employee monitors, and smartphones—already contributing to the Internet of Things. These devices are currently generating reams of data about their users' activities, habits, preferences, personalities, and characteristics. Those data are intensely valuable. At the same time, the Internet of Things presents new and difficult issues. Put most simply, this much new, high-quality data cannot enter the economy without the potential for misuse. To reap the benefits of the Internet of Things, we must deal proactively with its likely harms.

This Part explores four problems: (1) the reality that Big Data analysis of the Internet of Things will likely lead to unexpected inferences that cross contexts in potentially unacceptable and discriminatory ways; (2) the near impossibility of perfectly de-identifying Internet of Things data to protect privacy; (3) the vulnerability of these consumer devices to hacking and other security breaches; and (4) the weakness of consumer sensor privacy policies and of notice and choice in this context in which small, often screenless devices may generate a great deal of invisible data. For each issue—discrimination, privacy, security, and consent—I consider not only the technical problems inherent in the Internet of Things but the ways in which existing law is unprepared to address those problems.

A. Discrimination

The first Internet of Things problem is the Achilles' heel of widespread sensor deployment: Internet of Things data will allow us to sort consumers more precisely than ever before, but such sorting can easily turn from relatively benign differentiation into new and invidious types of unwanted discrimination. This subpart explores both the technical and legal problems of discrimination on the Internet of Things. The technical problem is simple: coupled with Big Data or machine learning analysis, massive amounts of sensor data from Internet of Things devices can give rise to unexpected inferences about individual consumers. Employers, insurers, lenders, and others may then make economically important decisions based on those inferences, without consumers or regulators having much understanding of that process. This could lead to new forms of illegal discrimination against those in protected classes such as race, age, or gender. More likely, it may create troublesome but hidden forms of economic discrimination based on Internet of Things data. Currently, both traditional discrimination law and information privacy law, such as the FCRA, are unprepared for such new forms of discriminatory decision making.

1. The Technical Problem: Sensor Fusion & Big Data Analytics May Mean That Everything Reveals Everything.—Consider an example. Imagine that a consumer uses a Fitbit fitness-tracking bracelet to monitor her fitness regime and overall health. In addition, she has an Internet-connected Aria scale—owned by Fitbit—that she uses to track her weight-loss progress. She has used these devices for several months, storing and viewing her information on Fitbit's web site. Our hypothetical consumer now decides to apply for a job—or a mortgage, loan, or insurance policy. During the application process her prospective employer interviews her and runs her through various tests, simulations, and other exercises to discern her experience, knowledge base, and ability to work well with others. As a final step in the hiring process, the employer asks for access to our candidate's Fitbit records from the previous three months.

Although this may seem outrageous, employers increasingly analyze various data about potential employees to discern who will be most productive, effective, or congenial. As one commentator recently put it: "[T]his . . . is the single biggest [Big Data] opportunity in business. If we can apply science to improving the selection, management, and alignment of people, the returns can be tremendous."[211] Such "talent analytics"[212] could increasingly incorporate sensor data from the Internet of Things. Employers have become more comfortable with using such devices as part of wellness programs.[213] Virgin Pulse, for example, offers a turnkey "pay-for-prevention" program to employers that integrates incentives with electronic pedometers, heart-rate monitors, and biometric tracking.[214] Some employers have also become more comfortable demanding such information from employees. In March 2013, for example, CVS Pharmacy announced that employees must submit information about their weight, body fat composition, and other personal health metrics on a monthly basis or pay a monthly fine.[215] It is not a big step to imagine employers incorporating such data into hiring as well.

---

211. Josh Bersin, *Big Data in Human Resources: Talent Analytics Comes of Age*, FORBES (Feb. 17, 2013, 8:00 PM), http://www.forbes.com/sites/joshbersin/2013/02/17/bigdata-in-human-resources-talent-analytics-comes-of-age/, *archived at* http://perma.cc/4R2A-LSMF.

212. *Id.*; *cf. Our Expertise*, EVOLV, http://www.evolv.net/expertise/, *archived at* http://perma.cc/E2T7-ZT3D (offering a human-resources predictive-analytics service to companies wishing to use big data to improve workforce hiring and productivity).

213. *See* Partrick J. Skerrett, *The Potential of Remote Health Monitoring at Work*, HBR BLOG NETWORK, HARV. BUS. REV. (Dec. 9, 2009, 2:34 PM), http://blogs.hbr.org/health-and-well-being/2009/12/the-potential-of-remote-health.html, *archived at* http://perma.cc/KX47-8CPN (tracking the positive trend of employers using Internet of Things data to track employees' health).

214. *See Our Wellness Solution*, VIRGIN PULSE, https://www.virginpulse.com/our-solution/our-wellness-solution, *archived at* http://perma.cc/P4WN-4SBZ (advertising a wellness program to companies that pairs wearable devices and mobile applications to track and improve employee health with a customizable incentives program).

215. Steve Osunsami, *CVS Pharmacy Wants Workers' Health Information, or They'll Pay a Fine*, ABC NEWS (Mar. 20, 2013, 7:43 AM), http://abcnews.go.com/blogs/health/2013/03/20/cvs-

Fitbit data could reveal a great deal to an employer. Impulsivity and the inability to delay gratification—both of which might be inferred from one's exercise habits—correlate with alcohol and drug abuse,[216] disordered eating behavior,[217] cigarette smoking,[218] higher credit-card debt,[219] and lower credit scores.[220] Lack of sleep—which a Fitbit tracks—has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear.[221] Such information could tip the scales for or against our hypothetical candidate.

The real issue, however, is not merely that an employer or other decision maker might demand access to such data. The technical problem created by the Internet of Things is that sensor data tend to combine in unexpected ways, giving rise to powerful inferences from seemingly innocuous data sources. Put simply, in a world of connected sensors, "everything may reveal everything." Sensor data are so rich, accurate, and fine-grained that data from any given sensor context may be valuable in a variety of—and perhaps all—other economic or information contexts.

Thus, an employer might not have to demand access to a candidate's Fitbit data. Individuals' driving data—from their EDR, after-market consumer automobile monitor, or insurance telematics device—could likewise give rise to powerful inferences about their personality and habits.

---

pharmacy-wants-workers-health-information-or-theyll-pay-a-fine, *archived at* http://perma.cc/VZ65-VNT8.

216. C.W. Lejuez et al., *Behavioral and Biological Indicators of Impulsivity in the Development of Alcohol Use, Problems, and Disorders*, 34 ALCOHOLISM: CLINICAL & EXPERIMENTAL RES. 1334, 1335 (2010).

217. Adrian Meule et al., *Enhanced Behavioral Inhibition in Restrained Eaters*, 12 EATING BEHAVIORS 152, 152–53 (2011).

218. *See* Nathasha R. Moallem & Lara A. Ray, *Dimensions of Impulsivity Among Heavy Drinkers, Smokers, and Heavy Drinking Smokers: Singular and Combined Effects*, 37 ADDICTIVE BEHAVIORS 871, 871 (2012) ("There has been much evidence that heavy drinkers . . . and smokers . . . have increased delay reward discounting, that is, impulsively choosing a smaller, immediate reward over a larger, delayed reward . . . ." (citations omitted)).

219. *See* Stephan Meier & Charles Sprenger, *Present-Biased Preferences and Credit Card Borrowing*, 2 AMER. ECON. J.: APPLIED ECONOMICS 193, 193, 195 (2010) (finding that individuals with a strong desire for immediate consumption consistently exhibit greater credit-card borrowing and have higher credit balances).

220. *See* Stephan Meier & Charles Sprenger, *Impatience and Credit Behavior: Evidence from a Field Experiment* 21 (Research Ctr. for Behavioral Econ. and Decision-Making, Fed. Reserve Bank of Bos., Paper No. 07-3, 2007), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=982398, *archived at* http://perma.cc/ZM9Q-LYTK ("[C]onfirming that more impatient individuals have lower credit scores . . . .").

221. *See, e.g.*, Seth Maxon, *How Sleep Deprivation Decays the Mind and Body*, ATLANTIC, Dec. 30, 2013, http://www.theatlantic.com/health/archive/2013/12/how-sleep-deprivation-decays-the-mind-and-body/282395/?single_page=true, *archived at* http://perma.cc/MQB5-U24S (discussing multiple studies documenting the adverse effects of sleep deprivation on physical and mental health); *Sleep, Performance, and Public Safety*, HEALTHYSLEEP, HARV. MED. SCH., http://healthysleep.med.harvard.edu/healthy/matters/consequences/sleep-performance-and-public-safety, *archived at* http://perma.cc/D3KE-EXQ7 ("Sleep deprivation negatively impacts our mood, our ability to focus, and our ability to access higher-level cognitive functions.").

Her electricity usage might similarly reveal much about her daily life, how late she typically arrived at home, and other traits that could be of interest. Her smartphone data could also be extremely revealing. As just one example of a surprising inference, research has shown that conversational patterns—listening, speaking, and quiet states—can be inferred from various types of sensors, including respiratory rates[222] and accelerometer data like that generated by a smartphone.[223] As discussed in subpart I(D), employers can learn a great deal about employees from such conversational information, even without recording audio of any kind.[224]

With so many potential data sources providing relevant information about a potential employee, an employer could turn to any number of commercial partners for information about that employee. One's mobile phone carrier, electric utility company, and auto insurer might have such useful information, as would the makers of the myriad Internet of Things products reviewed in Part I. The Internet has given rise to a massive infrastructure of data brokers that accumulate and track information about individuals. How long before they begin to incorporate the incredibly rich and revealing data from the Internet of Things?

The extent to which "everything reveals everything" is an empirical question, and one that my colleague Paul Ohm and I have begun to investigate experimentally.[225] It may be that some natural constraints remain between information types or uses and that certain sensor data do *not* correlate with or predict certain economically valuable traits. Fitness may not predict creditworthiness; driving habits may not predict employability. We don't know for sure. There is reason to expect, however, that everything may reveal everything *enough* to justify real concern. Consider two arguments for this prediction.

First, computer scientists have long discussed the phenomenon of "sensor fusion." Sensor fusion is the combining of sensor data from different sources to create a resulting set of information that is better than if the

---

222. *See* Md. Mahbubur Rahman et al., *mConverse: Inferring Conversation Episodes from Respiratory Measurements Collected in the Field*, *in* WIRELESS HEALTH 2011, at art. 10 (2011) ("[T]his is the first work to show that inference of listening state is possible from respiration measurements.").

223. *See* Aleksandar Matic et al., *Speech Activity Detection Using Accelerometer*, *in* 34TH ANNUAL INTERNATIONAL CONFERENCE OF THE IEEE MEDICINE AND BIOLOGY SOCIETY 2112, 2112 (2012) (measuring laryngeal vibrations with an accelerometer as a means of detecting speech patterns).

224. *Cf. id.* at 2114–15 (concluding that accelerometer data can provide information about a person's social activity without raising the privacy concerns associated with recording conversations).

225. *See generally* Scott Peppet & Paul Ohm, The Discriminatory Inferences Project (June 6, 2014) (unpublished manuscript) (on file with author). That research was presented at the Seventh Annual Privacy Law Scholars Conference. *June 2014 Privacy Law Scholars Conference*, BERKELEYLAW, http://www.law.berkeley.edu/plsc.htm, *archived at* http://perma.cc/G2S9-MZRR.

information is used separately.[226] A classic example is the creation of stereoscopic vision—including depth information—by combining the images of two offset cameras. A new piece of information—about depth—can be inferred from the combination of two other pieces of data, neither of which independently contains that new information.

The principle of sensor fusion means that data gleaned from various small sensors can be combined to draw much more complex inferences than one might expect. Data from an accelerometer and a gyroscope—both of which measure simple movements—can be combined to infer a person's level of relaxation (based on whether their movements are steady and even or shaky and tense).[227] If one adds heart-rate sensor data, one can readily infer stress levels and emotions, because research has shown that heart-rate variations from physical exercise have a different pattern than increases due to excitation or emotion.[228] Similarly, one might infer emotion or mental state from a variety of other daily activities, such as the way a consumer holds a cell phone, how smoothly a person types a text message, or how shaky a person's hands are while holding their phone.[229] Again, sensor fusion allows such complex and unexpected inferences to be drawn from seemingly simple data sources. As consumers use devices with more and different types of sensors—from fitness trackers to automobiles, ovens to workplace identification badges—these sensor data will fuse to reveal more and different things about individuals' behaviors, habits, and future intentions.

Second, Internet of Things data are ripe for Big Data or machine learning analysis:

> Networked body-worn sensors and those embedded in mobile devices we carry (e.g., smartphones) can collect a variety of measurements about physical and physiological states, such as acceleration, respiration, and ECG. By applying sophisticated machine learning algorithms to these data, rich inferences can be made about the physiological, psychological, and behavioral states and activities of people. Example inferences include dietary habits, psychosocial stress, addictive behaviors (e.g., drinking), exposures to

---

226. *See, e.g.*, David L. Hall & James Llinas, *An Introduction to Multisensor Data Fusion*, 85 PROC. IEEE 6, 6 (1997) ("In addition to the statistical advantage gained by combining same-source data . . . , the use of multiple types of sensors may increase the accuracy with which a quantity can be observed and characterized."). Sensor fusion is a subset of the general idea of data fusion, by which data from different sources is combined to draw new, more powerful inferences. *See id.* at 14–17 (proposing three alternative data-fusion architectures that incorporate multisensory data in different ways); Richard Beckwith, *Designing for Ubiquity: The Perception of Privacy*, IEEE PERVASIVE COMPUTING, Apr.–June 2003, at 40, 43 ("Data from various sensors can be merged to yield second-order data . . . . It's difficult to imagine various uses for fused data when you don't even consider that a fusion could take place.").

227. KAIVAN KARIMI, THE ROLE OF SENSOR FUSION AND REMOTE EMOTIVE COMPUTING (REC) IN THE INTERNET OF THINGS 6–7 (2013), *available at* http://cache.freescale.com/files/32bit/doc/white_paper/SENFEIOTLFWP.pdf, *archived at* http://perma.cc/FP82-HK55.

228. *Id.* at 6.

229. *Id.* at 7.

> pollutants, social context, and movement patterns. . . .
>
> . . . Seemingly innocuous data shared for one purpose can be used to infer private activities and behaviors that the individual did not intend to share.[230]

Commercial firms are already applying Big Data techniques to Internet of Things data to produce such inferences.

Consider, for example, the credit industry. I have explored elsewhere the evolution of credit scoring in the Internet age,[231] but suffice to say that lenders continually expand the types of information they incorporate into credit assessments. Most recently, some lenders have included data from social networks, such as Facebook and LinkedIn, to gauge credit risk.[232] Neo Finance, for example, targets auto-loan borrowers and uses social networks to gauge a borrower's credit risk,[233] as does Lenddo, a microlender in Hong Kong that uses social-network density to make credit decisions.[234] Similarly, the start-up Kreditech examines over fifteen thousand data points to create an alternative to FICO scores. These include location data; social data (e.g., likes, friends, locations, posts); e-commerce shopping behavior; and device data (e.g., apps installed, operating systems installed).[235] Kreditech focuses on consumers in emerging markets where traditional credit scores do not exist.[236]

In keeping with this search for more nuanced and predictive data sources, lenders are beginning to experiment with incorporating Internet of Things sensor data into such decisions. Cell-phone data are an obvious first place to start. For example, Safaricom, Kenya's largest cell-phone operator, studies its mobile phone users to establish their trustworthiness. Based on

---

230. Raij et al., *supra* note 49, at 11 (citations omitted).

231. *See* Peppet, *supra* note 48, 1163–64 (examining how credit companies, among other institutions, increasingly use the Internet to mine and aggregate data, profile consumers, and assess credit risk).

232. *See* Evelyn M. Rusli, *Bad Credit? Start Tweeting: Startups are Rethinking How to Measure Creditworthiness Beyond FICO*, WALL ST. J., Apr. 1, 2013, http://online.wsj.com/news/articles/SB10001424127887324883604578396852612756398, *archived at* http://perma.cc/5MJ5-TGDX (listing social-media factors considered by some lending companies); Evgeny Morozov, *Your Social Networking Credit Score*, SLATE (Jan. 30, 2013, 8:30 AM), http://www.slate.com/articles/technology/future_tense/2013/01/wonga_lenddo_lendup_big_data_and_social_networking_banking.html, *archived at* http://perma.cc/W5TW-4NXD (giving examples of various algorithms that use one's connections on social media as a factor in determining credit risk or worthiness).

233. Rusli, *supra* note 232 (detailing how Neo Finance analyzes customers' LinkedIn profiles when making loan decisions); *About*, NEO, https://neoverify.com/about, *archived at* http://perma.cc/U7LQ-3GNN.

234. *What Is Lenddo?*, LENDDO, https://www.lenddo.com/pages/what_is_lenddo/about, *archived at* http://perma.cc/7A2X-KTTC.

235. *The KrediTechnology*, KREDITECH, http://www.kreditech.com/#kreditechnology, *archived at* http://perma.cc/K265-9JR6. Similarly, Wonga, based in London, examines between 6,000 and 8,000 data points about potential customers. William Shaw, *Cash Machine: Could Wonga Transform Personal Finance?*, WIRED, May 5, 2011, http://www.wired.co.uk/magazine/archive/2011/06/features/wonga, *archived at* http://perma.cc/6R2M-HZKE.

236. *The KrediTechnology*, *supra* note 235.

how often its customers top up their airtime, for example, it may then decide to extend them credit.[237] Similarly, Cignifi uses the length, time of day, and location of cell calls to infer the lifestyle of smartphone users—and hence the reliability of those users—for loan applicants in the developing world.[238]

Sensor fusion and Big Data analysis combine to create the possibility that everything reveals everything on the Internet of Things. Although a consumer may use a Fitbit solely for wellness-related purposes, such data could easily help an insurer draw inferences about that consumer to set premiums more accurately (e.g., amount of exercise may influence health or life insurance, or amount and quality of sleep may influence auto insurance); aid a lender in assessing the consumer's creditworthiness (e.g., conscientious exercisers may be better credit risks); help an employer determine whom to hire (e.g., those with healthy personal habits may turn out to be more diligent employees); or even help a retailer price discriminate (e.g., those wearing a Fitbit may have higher incomes than those without). To the extent that context-violative data use breaks privacy norms—as Helen Nissenbaum and others have argued—consumer sensors will disrupt consumers' expectations.[239] This is Big Data at an entirely new scale, brought about by the proliferation of little sensors.[240]

2. The Legal Problem: Antidiscrimination and Credit Reporting Law Is Unprepared.—There are two main legal implications of the possibility that everything may begin to reveal everything. First, will the Internet of Things lead to new forms of discrimination against protected classes, such as race? Second, will the Internet of Things lead to troubling forms of economic discrimination or sorting?

a. Racial & Other Protected Class Discrimination.—If the Internet of Things creates many new data sources from which unexpected inferences can be drawn, and if those inferences are used by economic actors to make decisions, one can immediately see the possibility of seemingly innocuous

---

237. *See* ALICE T. LIU & MICHAEL K. MITHIKA, USAID, MOBILE BANKING–THE KEY TO BUILDING CREDIT HISTORY FOR THE POOR? 3 (2009), *available at* http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2012/03/mobile_banking_key_to_building_credit_history1.pdf, *archived at* http://perma.cc/6W9-L3PT (analyzing how M-PESA, Safaricom's mobile payment and mobile banking system, extends credit to users without formal banking or credit histories on the basis of mobile transactions and payment histories).

238. *How It Works*, CIGNIFI™, http://cignifi.com/en-us/technology, *archived at* http://perma.cc/G2WA-7PBW.

239. Heather Patterson & Helen Nissenbaum, Context-Dependent Expectations of Privacy in Self-Generated Mobile Health Data 43–45 (June 6, 2013) (unpublished manuscript) (on file with author). That paper was presented at the Sixth Annual Privacy Law Scholars Conference. *June 2013 Privacy Law Scholars Conference*, BERKELEYLAW, http://www.law.berkeley.edu/14524.htm, *archived at* http://perma.cc/QDP2-SVDL.

240. *See generally* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL CHANGE HOW WE LIVE, WORK, AND THINK (2013) (exploring the growing predictive, analytic, and commercial role of large-scale data use in society).

data being used as a surrogate for racial or other forms of illegal discrimination. One might not know a credit applicant's race, but one might be able to guess that race based on where and how a person drives, where and how that person lives, or a variety of other habits, behaviors, and characteristics revealed by analysis of data from a myriad of Internet of Things devices. Similarly, it would not be surprising if various sensor devices—a Fitbit, heart-rate tracker, or driving sensor, for example—could easily discern a user's age, gender, or disabilities. If sensor fusion leads to a world in which "everything reveals everything," then many different types of devices may reveal sensitive personal characteristics. As a result, the Internet of Things may make possible new forms of obnoxious discrimination.

This is a novel problem and one that legal scholars are just beginning to recognize.[241] I am not convinced that the most blatant and obnoxious forms of animus-based discrimination are likely to turn to Internet of Things data—if a decision maker wants to discriminate based on race, age, or gender, they likely can do so without the aid of such Internet of Things informational proxies. Nevertheless, the problem is worth considering because traditional antidiscrimination law is in some ways unprepared for these new forms of data.

Racial and other forms of discrimination are obviously illegal under Title VII.[242] Title I of the Americans with Disabilities Act (ADA) forbids discrimination against those with disabilities,[243] and the Genetic Information Nondiscrimination Act (GINA) bars discrimination based on genetic inheritance.[244] These traditional antidiscrimination laws leave room, however, for new forms of discrimination based on Internet of Things data. For example, nothing prevents discrimination based on a potential

241. *See, e.g.*, Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. ON TELECOMM. & HIGH TECH. L. 351, 358 (2013) (explaining that detecting discrimination based on Internet of Things data may be difficult since such discrimination may be based upon a large number of facially neutral factors). Some have argued that increased information about consumers may *dampen* discrimination against those in protected classes. Lior Strahilevitz is most known for taking this optimistic view that increased data flows will *curb* racial discrimination by allowing individuals and firms to discriminate for economically relevant reasons rather than using race, age, gender, or other protected classes as a discriminatory proxy. *See* Lior Jacob Strahilevitz, *Privacy Versus Antidiscrimination*, 75 U. CHI. L. REV. 363, 380 (2008) (supporting the publication of previously private information in an effort to discourage employers from using more subtle and unfavorable statistical discrimination techniques to avoid undesirable employees); Lior Jacob Strahilevitz, *Toward A Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2029 (2013) [hereinafter Strahilevitz, *Positive Theory*] ("[I] have argued that protecting privacy seems to thwart price and service discrimination while fostering statistical discrimination on the basis of race and gender . . . ."). *But see* Anita L. Allen, *Privacy Law: Positive Theory and Normative Practice*, 126 HARV. L. REV. F. 241, 245–46 (2013) (countering that even if increased information benefits some African Americans, such heavy surveillance might also create disproportionate burdens for African Americans as a group).

242. *See* 42 U.S.C. § 2000e–2(a) (2012) (prohibiting an employer from discriminating against prospective or current employees on the basis of "race, color, religion, sex, or national origin").

243. *Id.* § 12112(a).

244. *Id.* § 2000ff–4(a).

employee's health status, so long as the employee does not suffer from what the ADA would consider a disability.[245] Similarly, antidiscrimination law does not prevent economic sorting based on our personalities, habits, and character traits.[246] Employers are free not to hire those with personality traits they don't like; insurers are free to avoid insuring—or charge more to—those with risk preferences they find too expensive to insure; lenders are free to differentiate between borrowers with traits that suggest trustworthiness versus questionable character.[247]

As analysis reveals more and more correlations between Internet of Things data, however, this exception or loophole in antidiscrimination law may collapse under its own weight. A decision at least facially based on conduct—such as not to hire a particular employee because of her lack of exercise discipline—may systematically bias an employer against a certain group if that group does not or cannot engage in that conduct as much as others. Moreover, seemingly voluntary "conduct" may shade into an immutable trait depending on our understanding of genetic predisposition. Nicotine addiction and obesity, for example, may be less voluntary than biologically determined.[248] The level of detail provided by Internet of Things data will allow such fine-grained differentiation that it may easily begin to resemble illegal forms of discrimination. Currently, traditional antidiscrimination law has not yet considered these problems.

b. Economic Discrimination.—Even without the problem of race, age, or gender discrimination, using Internet of Things data to discriminate between—or "sort"—consumers is also potentially controversial. If widespread consumer sensor use leads to a world in which everything reveals everything, this will permit insurers, employers, lenders, and other economic actors to distinguish more finely between potential insureds, employees, and borrowers. From the perspective of economics, this may be beneficial. Put simply, more data will allow firms to separate pooling equilibria in insurance, lending, and employment markets, leading to efficiencies and increased

245. *See* Jessica L. Roberts, *Healthism and the Law of Employment Discrimination*, 99 IOWA L. REV. 571, 595–97 (2014) (analyzing whether being overweight or obese would qualify as an impairment protected under the ADA).

246. *See* Strahilevitz, *Postive Theory*, *supra* note 241, at 2024 ("Maybe the law's tolerance for personality discrimination ought to be questioned, but American antidiscrimination law presently does not regard that kind of question as close."). There is some debate about whether an employer conducting a personality test on a potential employee triggers the ADA's prohibition on pre-job-offer medical examinations. *See* Gregory R. Vetter, Comment, *Is a Personality Test a Pre-Job-Offer Medical Examination Under the ADA?*, 93 NW. U. L. REV. 597, 598–99 (1999) (noting that courts have inconsistently ruled on whether personality tests qualify as prohibited medical examinations under the ADA).

247. *See* Roberts, *supra* note 245, at 604–05 (comparing trait-based and conduct-based discrimination and explaining why the ADA covers the former but not the latter).

248. *See id.* at 614–15 (identifying research studies suggesting that obesity and nicotine addiction may not be exclusively voluntary traits).

social welfare.[249] From a legal or policy perspective, however, economic sorting is just not that simple. The public and its legislators tend to react strongly to forms of economic discrimination that economists view as relatively benign. For example, price discrimination—charging one consumer more for a good than another because of inferences about the first person's willingness or ability to pay—may be economically neutral or even efficient, but consumers react strongly against it.[250]

As indicated, traditional antidiscrimination law does not forbid differentiating between individuals on the basis of their behavior, personality, or conduct. That said, some constraints do exist on the use of Internet of Things data streams for such inferences and purposes. Most important, the FCRA establishes consumers' rights vis-à-vis credit reports.[251] Under the FCRA, "consumer reporting agenc[ies]" (CRAs) are entities that engage in "assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ."[252] A consumer report is any report

> of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used . . . for the purpose of serving as a factor in establishing the consumer's eligibility for—
>
> (A) credit or insurance . . . ; [or]
>
> (B) employment purposes . . . .[253]

The FTC has warned mobile-application developers that if they provide information to employers about an individual's criminal history, for example, they may be providing consumer reports and thus regulated by the FCRA.[254]

---

249. *See* Strahilevitz, *Positive Theory*, *supra* note 241, at 2021 (illustrating how companies determine a person's credit risk or potential purchase decisions based on seemingly unrelated factors, such as whether the person has purchased felt pads for furniture).

250. *See, e.g.*, Alessandro Acquisti & Hal R. Varian, *Conditioning Prices on Purchase History*, 24 MARKETING SCI. 367, 367–68, 380 (2005) (discussing ways consumers seek to avoid a company tracking their purchase or behavioral history but concluding that, as transactions become increasingly computerized, the use of customers' behavioral or purchase data may increase consumer welfare); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 996, 1026–27 (2014) (postulating that some consumers would incur additional transaction costs just to avoid disclosing behavioral or personal data to companies). *But see* Ariel Porat & Lior Jacob Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data*, 112 MICH. L. REV. 1417, 1456 (2014) (suggesting that the effect of price discrimination on consumer welfare may be more ambiguous than indicated by some scholars).

251. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012).

252. *Id.* § 1681a(f).

253. *Id.* § 1681a(d)(1).

254. On January 25, 2012, the FTC sent warning letters to three marketers of mobile applications (Everify, InfoPay, and Intelligator) that provided criminal background checks to employers. Letter from Maneesha Mithal, Assoc. Dir., Fed. Trade Comm'n, to Alon Cohen, Everify, Inc. (Jan. 25, 2012), http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting-act/120207everifyletter.pdf, *archived at* http://perma.cc/7BXC-W68A; Letter from Maneesha Mithal, Assoc. Dir., Fed. Trade

By analogy, if a consumer sensor company such as Fitbit began to sell their data to prospective employers or insurance companies, the FTC could take the position that Fitbit had become a CRA under the FCRA. If a company such as Fitbit were classified as a CRA, consumers would have the right to dispute the accuracy of any information provided by such a CRA.[255] If Internet of Things manufacturers were *not* deemed CRAs, but instead deemed to be providing information *to* CRAs—such as established credit-reporting firms or data aggregators—the FCRA would forbid Internet of Things firms from knowingly reporting inaccurate information and would require that such firms correct and update incomplete or incorrect information.[256]

Although this somewhat constrains the use of Internet of Things data streams, the FCRA's reach is limited. First and foremost, a lender, insurer, or employer doing its *own* analysis of sensor data would not trigger the FCRA's CRA-related requirements.[257] Thus, Internet of Things data could be requested from applicants or gathered by such firms with impunity, as in the introductory example to this section.

Further, the FCRA does not apply if data are used to tailor *offers* made through sophisticated electronic marketing techniques.[258] For example, if a data aggregator sells a consumer's profile—including a profile based on Internet of Things sensor data—to a credit-card company at the moment that the consumer accesses the credit-card company's website, and that profile is used to tailor what the consumer sees on the website (e.g., displaying one or

---

Comm'n, to Daniel Dechamps, InfoPay, Inc. (Jan. 25, 2012), http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting-act/120207infopayletter.pdf, *archived at* http://perma.cc/F3PV-Z8VW; Letter from Maneesha Mithal, Assoc. Dir., Fed. Trade Comm'n, to Amine Mamoun, Intelligator, Inc. (Jan. 25, 2012), http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting-act/120207intelligatorletter.pdf, *archived at* http://perma.cc/Y5BJ-CJU2.

255. *See* 15 U.S.C. § 1681i(a)(1)(A) (providing that a consumer may dispute the accuracy of any item of information in a consumer reporting agency's file and requiring an agency to conduct a "reasonable reinvestigation" to determine the accuracy of and potentially correct the contested information).

256. *See id.* §1681s–2(a)(1)(A)–(B) (providing that a person may not knowingly provide any inaccurate consumer information to a consumer reporting agency).

257. *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the 23d Computers Freedom and Privacy Conference: Reclaim Your Name 4 (June 26, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf, *archived at* http://perma.cc/J3HA-U2HN (describing "new-fangled lending institutions" that use in-house credit reports derived from Big Data analyses, which practice "falls right on—or just beyond—the boundaries of FCRA"); *see also* Nate Cullerton, Note, *Behavioral Credit Scoring*, 101 GEO. L.J. 807, 827 (2013) ("[T]he FCRA appears not to apply at all to credit determinations made 'in house' by credit issuers if they are not based on a credit report.").

258. *See* Brill, *supra* note 257, at 4 ("It can be argued that e-scores don't yet fall under FCRA because they are used for marketing and not for determinations on ultimate eligibility.").

another credit card based on assumptions about that consumer), that tailored offer does not trigger the FCRA's provisions.[259]

Finally, the FCRA is designed to ensure *accuracy* in credit reports. The FCRA gives consumers the right to check and challenge the accuracy of information found in such reports so that credit, insurance, and employment determinations are fair.[260] Accuracy, however, is really not the problem with Internet of Things sensor data. One's Fitbit, driving, or smart home sensor data are inherently accurate—there is little to challenge. What is more questionable are the inferences *drawn* from such data. The FCRA does not reach those inferences, however. It applies to the underlying "inputs" into a credit, insurance, or employment determination, not the reasoning that a bank, insurer, or employer then makes based on those inputs.[261] Thus, the FCRA provides consumers with little remedy if Internet of Things data were to be incorporated into credit-reporting processes.

In summary, both traditional antidiscrimination law and data-use-related legislation such as the FCRA are unprepared to address the problem that, on the Internet of Things, everything may reveal everything.

B. Privacy

Discrimination based on sensor data is a potential problem so long as individualized inferences can be drawn from sensor data: if *your* Fitbit or automotive or smartphone data are used to draw inferences about *you*. One solution would be to simply aggregate and anonymize all such data, refusing to release information about particular individuals. Many manufacturers of consumer sensor devices take this approach, promising users that their data will only be shared with others in de-identified, anonymous ways.[262] Does this solve the problem of discrimination and protect consumers' privacy?

1. The Technical Problem: Sensor Data Are Particularly Difficult to De-Identify.—Unfortunately not. Return to our Fitbit example. Even were Fitbit to de-identify its information by removing a user's name, address, and other obviously identifying information from the dataset before it shared that information with others, it would be relatively easy to *re*-identify that dataset. The reason is straightforward: each of us has a unique gait. This means that if I knew something about an individual Fitbit user's gait or style of walking,

---

259. Cullerton, *supra* note 257, at 827 (arguing that such offers do not trigger the FCRA so long as the data are not used to make an "actual lending decision").

260. 15 U.S.C. § 1681i(a)(1)(A).

261. *See id.* § 1681s–2(a)(1)(A)–(B), (2) (prohibiting anyone from knowingly providing inaccurate information to CRAs and creating a duty to correct inaccurate information already provided to a CRA).

262. *E.g.*, *Fitbit Privacy Policy*, FITBIT, http://www.fitbit.com/privacy#DataSharedWithThirdParties, *archived at* http://perma.cc/MG2N-6DWX ("We only share data about you when it is necessary to provide our services, when the data is de-identified and aggregated, or when you direct us to share it.").

I could use that information to identify that individual among the millions of anonymized Fitbit users' data. I would then have access to all of that user's *other* Fitbit data, which would now be re-associated with her. As Ira Hunt, Chief Technology Officer of the Central Intelligence Agency, put it: "[S]imply by looking at the data [from a Fitbit] they can find out . . . with pretty good accuracy what your gender is, whether you're tall or you're short, whether you're heavy or light, . . . [and] you can be 100% . . . identified by simply your gait—how you walk."[263]

In the last five years, legal scholars have become increasingly wary of the extent to which large datasets can ever be truly anonymized. My colleague Paul Ohm has argued that advances in computer science increasingly make it possible to attack and re-identify supposedly "anonymized" databases, rendering futile many attempts to protect privacy with anonymity.[264] Without delving into the burgeoning literature on de-identification generally, the point here is that *sensor* datasets are particularly vulnerable.[265]

Anonymization or de-identification becomes exceedingly difficult in sparse datasets: datasets in which an individual can be distinguished from other individuals by only a few attributes.[266] Sensor datasets are particularly prone to sparsity.[267] The reason is simple: sensor data capture such a rich picture of an individual, with so many related activities, that each individual in a sensor-based dataset is reasonably unique.[268] For example, if a health sensor captures an individual's movements throughout the day, it is quite easy to infer what types of transportation that individual used (e.g., car, bike, or subway). That unique pattern of transportation uses, however, means that

---

263. Ira Hunt, Chief Tech. Officer, Cent. Intelligence Agency, Address at Gigaom Structure Data 2013: The CIA's Grand Challenges with Big Data (Mar. 20, 2013), *available at* http://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data/2, *archived at* http://perma.cc/Q8DG-S2PL.

264. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703–04 (2010) (asserting that promises of data privacy through de-identification are "illusory" in light of advances in re-identification and that "[d]ata can be either useful or perfectly anonymous but never both") (emphasis omitted). *But see* Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 3–4 (2011) (countering that Ohm misinterpreted prior literature and research and overstated the "futility of anonymization").

265. *See* Raij et al., *supra* note 49, at 13 ("[E]xisting anonymization techniques alone cannot be used to protect individuals sharing personal sensor data.").

266. *See generally* Nicholas D. Lane et al., *On the Feasibility of User De-Anonymization from Shared Mobile Sensor Data*, *in* PHONESENSE '12: PROCEEDINGS OF THE THIRD INTERNATIONAL WORKSHOP ON SENSING APPLICATIONS ON MOBILE PHONES, at art. 3 (2012) (studying how methods for leveraging sparse datasets could be used to de-identify shared mobile sensor data gleaned from smartphones).

267. *See id.* (studying mobile sensor datasets, which are prone to sparsity because mobile sensors measure a mixture of "infrequently occurring events" over an extended period of time).

268. In addition to the fact that sensor data tend to be sparse, sensors themselves are also unique. An individual sensor may produce a unique fingerprint of "noise" that can then identify that sensor. For example, digital cameras can be individually identified from the patterns of sensor noise that they generate. Jan Lukáš et al., *Digital Camera Identification from Sensor Pattern Noise*, 1 IEEE TRANSACTIONS ON INFO. FORENSICS & SECUR. 205, 205 (2006).

if I have access to that anonymized dataset containing your complete sensor information, and if I simultaneously know a few specific dates and times that you rode the subway or a bike, for example, I can probably determine which of the many users in that dataset you are—and therefore know *all* of your movement information for all dates and times.[269]

Preliminary research suggests that robust anonymization of Internet of Things data is extremely difficult to achieve, or, put differently, that re-identification is far easier than expected:

> [R]esearchers are discovering location-oriented sensors are not the only source of concern and finding other sensors modalities can also introduce a variety of new privacy threats . . . . [S]ensors, such as accelerometers, gyroscopes, magnetometers, or barometers, which at first glance may appear innocuous, can lead to significant new challenges to user anonymization.[270]

For example, researchers at MIT recently analyzed data on 1.5 million cell-phone users in Europe over fifteen months and found that it was relatively easy to extract complete location information about a single person from an anonymized dataset containing more than a million people.[271] In a stunning illustration of the problem, they showed that to do so required only locating that single user within several hundred yards of a cell-phone transmitter sometime over the course of an hour on four occasions in one year.[272] With four such known data points, the researchers could identify ninety-five percent of the users in the dataset.[273] As one commentator on this landmark study put it: for sensor-based datasets, "it's very hard to preserve anonymity."[274]

Consider another example. Many smartphone owners are concerned about the misuse of their location data, which is often considered quite sensitive. In addition to GPS location sensors, however, most smartphones contain an accelerometer that measures the ways in which the smartphone is

---

269. *See* Lane et al., *supra* note 266 (explaining how mobile sensors will capture everyday user activities, such as commuting, which are affected by "high-level user characteristics and restraints" and increase the likelihood for relationships to exist between otherwise unrelated activities).

270. Lane et al., *supra* note 266 (citations omitted); *see also* Mudhakar Srivatsa & Mike Hicks, *Deanonymizing Mobility Traces: Using Social Networks as a Side-Channel*, *in* CCS'12: THE PROCEEDINGS OF THE 2012 ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 628, 628 (2012) (examining how one's social network may be used to deanonymize personally identifying information).

271. Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, SCI. REP., Mar. 25, 2013, at 4, 4; *see also* Sébastien Gambs et al., *De-Anonymization Attack on Geolocated Datasets*, 80 J. COMP. & SYS. SCI. 1597, 1597 (2014) (describing how a mobility-trace dataset potentially can be used to infer an individual's points of interest; past, current, and future movements; and social network).

272. Montjoye et al., *supra* note 271, at 2 & fig.1.

273. *Id.* at 2.

274. Larry Hardesty, *How Hard Is It to "De-Anonymize" Cellphone Data?*, MIT NEWS (Mar. 27, 2013), http://newsoffice.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data, *archived at* http://perma.cc/76PS-8SXH.

moving through space. Research shows that the data emitted by an accelerometer from one smartphone can often be correlated with similar data from a second phone to reveal that the two phones are producing sufficiently similar motion signatures to support the inference that they are in the same location.[275] In addition, if a smartphone user is driving her car, the patterns of acceleration and motion created by the car moving over the roadway are unique as to any other location.[276] As the authors of the study revealing this finding put it: "[T]he idiosyncrasies of roadways create globally unique constraints. . . . [T]he accelerometer can be used to infer a location with no initial location information."[277] So long as one phone (with a known location) has travelled the same roads as the previously "hidden" phone (with unknown location), the latter can be located.

2. The Legal Problem: Privacy Law Is Unprepared.—The inherent sparsity of Internet of Things data means that protecting privacy through anonymization is particularly unlikely to succeed. The legal implications are dramatic. Ohm has catalogued the huge number of privacy laws that rely on anonymization.[278] Many distinguish "personally identifiable information" (PII)—usually defined as name, address, social-security number, or telephone number—from other data that is presumed not to reveal identity.[279] The threat of re-identification of sparse sensor-based datasets makes questionable this distinction between PII and other data.

Information-privacy scholarship has begun to debate how to address the threat of re-identification. Ohm proposes abandoning the idea of PII completely;[280] Paul Schwartz and Daniel Solove have recently resisted this approach, arguing instead that we should redefine PII along a continuum between identified information, identifiable information, and non-identifiable information.[281] The "identified" category pertains to information that is clearly associated with an individual.[282] The "non-identifiable" pertains to information that carries only a very "remote risk" of connection to an individual.[283] In the middle are data streams for which there is a non-trivial possibility of future re-identification.[284] Schwartz and Solove argue

---

275. Jun Han et al., *ACComplice: Location Inference Using Accelerometers on Smartphones*, *in* 2012 FOURTH INTERNATIONAL CONFERENCE ON COMMUNICATION SYSTEMS AND NETWORKS (COMSNETS 2012), at art. 25 (2012).

276. *Id.*

277. *Id.*

278. *See* Ohm, *supra* note 264, at 1740–41 (emphasizing that nearly every U.S. privacy statute relies on the presumptive validity of anonymization).

279. *Id.* at 1740–42.

280. *Id.* at 1742.

281. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1877 (2011).

282. *Id.*

283. *Id.* at 1878.

284. *Id.*

that the law should treat differently information in these three categories. For merely identifiable information that has not yet been associated with an individual, "[f]ull notice, access, and correction rights should *not* be granted."[285] In addition, "limits on information use, data minimalization, and restrictions on information disclosure should not be applied across the board to identifiable information."[286] Data security, however, should be protected when dealing with identifiable information.[287]

Others have adopted a similar approach.[288] According to the FTC, three considerations are most relevant: "as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the [FTC's proposed] framework."[289] The FTC is trying to distinguish, in short, between data that are "reasonably identifiable" and data that are not, as well as between firms that are taking reasonable steps to prevent re-identification.

Although Schwartz and Solove—and the FTC—are trying to use this new, third category of identifiable information to prevent the complete conceptual collapse of all data into the category of PII, that collapse may be inevitable in the Internet of Things context. If sensor datasets are so sparse that easy re-identification is the norm, then *most* Internet of Things data may be "reasonably identifiable." The FTC's standard—and the Schwartz and Solove solution—may mean that in the end all biometric and sensor-based Internet of Things data need to be treated as PII. That, however, would require a radical re-working of current law and practice. As we will see below, Internet of Things firms currently try to treat sensor data as "non-personal."[290] Corporate counsel, regulators, and legislators have not yet faced the reality that Internet of Things sensor data may all be identifiable. In short, privacy law—both on the books and on the ground—is unprepared for the threats created by the Internet of Things.

C. Security

Internet of Things devices suffer from a third problem: they are prone to security vulnerabilities for reasons that may not be simple to remedy. More importantly, data security laws—particularly state data-breach notification statutes—are unprepared for and don't apply to such security problems. To return to our example, if Fitbit's servers were hacked today,

---

285. *Id.* at 1880.

286. *Id.*

287. *Id.* at 1881.

288. *See* Tene & Polonetsky, *supra* note 19, ¶ 48 (criticizing the dichotomous approach for leading to an "arms race between de-identifiers and re-identifiers").

289. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 22 (2012).

290. *See supra* subsection II(D)(1)(b).

the company would have no legal obligation to inform the public and no legal consequence would likely attach.

1. The Technical Problem: Internet of Things Devices May Be Inherently Prone to Security Flaws.—The Internet of Things has recently begun to attract negative attention because of increasing concerns over data security. In November 2013, security firm Symantec discovered a new Internet worm that targeted small Internet of Things devices—particularly home routers, smart televisions, and Internet-connected security cameras—in addition to traditional computers.[291] In the first large-scale Internet of Things security breach, experts estimate that the attack compromised over one-hundred-thousand devices—including smart televisions, wireless speaker systems, and refrigerators—and used them to send out malicious e-mails.[292]

Although attention to such issues is on the rise, computer-security experts have known for years that small, sensor-based Internet of Things devices are prone to security problems.[293] A team from Florida International University showed that the Fitbit fitness tracker could be vulnerable to a variety of security attacks, and that simple tools could capture data from any Fitbit within 15 feet.[294] The device simply was not engineered with data security in mind.[295] In July 2014, Symantec released the results of a study of fitness trackers showing "security risks in a large number of self-tracking devices and applications."[296]

More dire, insulin pumps have been shown to be vulnerable to hacking. Jay Radcliffe, a security researcher with diabetes, has demonstrated that these

---

291. Kaoru Hayashi, *Linux Worm Targeting Hidden Devices*, SYMANTEC (Nov. 27, 2013, 11:53 AM), http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices, *archived at* http://perma.cc/UL7S-9BWJ.

292. Press Release, Proofpoint, Proofpoint Uncovers Internet of Things (IoT) Cyberattack (Jan. 16, 2014), http://www.proofpoint.com/about-us/press-releases/01162014.php, *archived at* http://perma.cc/M78W-VELZ.

293. For a useful interview related to this question, see Gigoam Internet of Things Show, *Securing the Internet of Things is Like Securing our Borders. Impossible*, SOUNDCLOUD (May 29, 2013), https://soundcloud.com/gigaom-internet-of-things/securing-the-internet-of, *archived at* http://perma.cc/J6V-WFEU and Daniela Hernandez, *World's Health Data Patiently Awaits Inevitable Hack*, WIRED, Mar. 25, 2013, http://www.wired.com/2013/03/our-health-information/, *archived at* http://perma.cc/JCU6-4EB5 (noting that security breaches related to healthcare information have increased and predicting that healthcare data repositories will be hacked in the future).

294. Mahmudur Rahman et al., Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device 1 (Apr. 20, 2013) (unpublished manuscript), *available at* http://arxiv.org/abs/1304.5672, *archived at* http://perma.cc/8W4D-6DBA.

295. *Cf.* Hunt, *supra* note 263 ("You guys know the Fitbit, right? It's just a simple 3-axis accelerometer. [The CIA] like[s] these things because they don't have any – well, I won't go into that . . . .").

296. *How Safe Is Your Quantified Self? Tracking, Monitoring, and Wearable Tech*, SYMANTEC (July 30, 2014, 2:27:53 PM), http://www.symantec.com/connect/blogs/how-safe-your-quantified-self-tracking-monitoring-and-wearable-tech, *archived at* http://perma.cc/4N7Y-PKJU.

medical devices can be remotely accessed and controlled by a hacker nearby the device's user.[297] Similarly, many insulin pumps communicate wirelessly to a small monitor that patients use to check insulin levels.[298] Radcliffe has shown that these monitors are also easily accessed, leading to the possibility that a malicious hacker could cause a monitor to display inaccurate information, causing a diabetic patient to mis-administer insulin doses.[299] Other medical devices have also proven insecure.[300]

As a final example, in August 2013, a Houston couple heard the voice of a strange man cursing in their two-year-old daughter's bedroom.[301] When they entered the room, the voice started cursing them instead.[302] The expletives were coming from their Internet-connected and camera-equipped baby monitor, which had been hacked.[303] Many other webcam devices have also been found vulnerable: in September 2013, the FTC took its first action against an Internet of Things firm when it penalized TRENDnet—a web-enabled camera manufacturer—for promising customers that its cameras were secure when they were not.[304]

These examples illustrate the larger technical problem: Internet of Things devices may be inherently vulnerable for several reasons. First, these products are often manufactured by traditional consumer-goods makers rather than computer hardware or software firms. The engineers involved may therefore be relatively inexperienced with data-security issues, and the firms involved may place insufficient priority on security concerns.[305]

---

297. Jordan Robertson, *Insulin Pumps, Monitors Vulnerable to Hacking*, YAHOO! NEWS (Aug. 5, 2011, 12:04 PM), http://news.yahoo.com/insulin-pumps-monitors-vulnerable-hacking-100605899.html, *archived at* http://perma.cc/RJ64-2GNW.

298. *Id.*

299. *Id.*

300. *Home, Hacked Home*, ECONOMIST, July 12, 2014, http://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home, *archived at* http://perma.cc/WW5Y-BDHM (noting various examples of medical equipment with security vulnerabilities).

301. Alana Abramson, *Baby Monitor Hacking Alarms Houston Parents*, ABCNEWS (Aug. 13, 2013, 12:43 PM), http://abcnews.go.com/blogs/headlines/2013/08/baby-monitor-hacking-alarms-houston-parents/, *archived at* http://perma.cc/UZ27-ZSUP.

302. *Id.*

303. *Id.*; *see also Home, Hacked Home*, *supra* note 300 (describing an Ohio couple's similar incident).

304. *See* TRENDnet, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 78 Fed. Reg. 55,717, 55,718–19 (Sept. 11, 2013) (describing the complaint against, and subsequent consent order with, TRENDnet); Press Release, Fed. Trade Comm'n, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles, *archived at* http://perma.cc/BYD4-HSSE.

305. *See* Brian Fung, *Here's the Scariest Part About the Internet of Things*, SWITCH, WASH. POST (Nov. 19, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/heres-the-scariest-part-about-the-internet-of-things/, *archived at* http://perma.cc/9ME3-2CAE ("Although the folks who make dishwashers may be fantastic engineers, or even great computer programmers, it doesn't necessarily imply they're equipped to protect Internet users from the outset.").

Second, consumer sensor devices often have a very compact form factor. The goal is to make a small health monitor that fits on your wrist or a health monitor that resides in the sole of your shoe. Small form factors, however, do not necessarily lend themselves to adding the processing power needed for robust security measures such as encryption.[306] In addition, small devices may not have sufficient battery life to support the extra processing required for more robust data security.

Finally, these devices are often not designed to be retooled once released into the market. A computer or smartphone contains a complex operating system that can be constantly updated to fix security problems, therefore providing a manufacturer with ongoing opportunities to secure the device against new threats. A consumer sensor device, however, is often less malleable and robust. Internet of Things products may thus not be patchable or easy to update.[307]

For all of these reasons, the Internet of Things may be inherently prone to security flaws. The risks go beyond spam. In addition to using these devices as remote servers, there are also endless possibilities for hacking into sensor-based devices for malicious purposes. As computer-security expert Ross Anderson recently asked: "What happens if someone writes some malware that takes over air conditioners, and then turns them on and off remotely? . . . You could bring down a power grid if you wanted to."[308] One could also, of course, spy on an individual's sensor devices, steal an individual's data, or otherwise compromise an individual's privacy. These problems have led some computer security experts to conclude that "without strong security foundations, attacks and malfunctions in the [Internet of Things] will outweigh any of its benefits."[309]

2. The Legal Problem: Data Security Law Is Unprepared.—Data security law is unprepared for these Internet of Things security problems. Data security in the United States is generally regulated through one of two mechanisms: FTC enforcement or state data-breach notification laws. Neither is clearly applicable to breaches of Internet of Things data. Put differently, if your biometric data were stolen from a company's servers, it is

306. *See* Stacey Higginbotham, *The Internet of Things Needs a New Security Model. Which One Will Win?*, GIGAOM (Jan. 22, 2014, 8:26 AM), http://gigaom.com/2014/01/22/the-internet-of-things-needs-a-new-security-model-which-one-will-win/, *archived at* http://perma.cc/9BXA-LA48 (explaining that because many connected devices have little computational power, security must be lightweight and tasks such as encryption are impossible).

307. Michael Eisen, *The Internet of Things is Wildly Insecure—And Often Unpatchable*, WIRED, Jan. 6, 2014, http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/, *archived at* http://perma.cc/X7H7-UBA5.

308. *Spam in the Fridge: When the Internet of Things Misbehaves*, ECONOMIST, Jan. 25, 2014, http://www.economist.com/news/science-and-technology/21594955-when-internet-things-misbehaves-spam-fridge, *archived at* http://perma.cc/HNG6-W8W4.

309. Rodrigo Roman et al., *Securing the Internet of Things*, COMPUTER, Sept. 2011, at 51, 51.

contestable whether any state or federal regulator would have the authority to respond.

First, consider the FTC's authority. Because there is no general federal data-security statute,[310] the FTC has used its general authority under the Federal Trade Commission Act (FTC Act) to penalize companies for security lapses.[311] The FTC Act states that "unfair or deceptive acts or practices in or affecting commerce" are unlawful.[312] The FTC has used both the unfair and deceptive prongs of the FTC Act to regulate privacy and security, generally through consent orders with offending firms.[313] In "deception" cases—such as the 2013 TRENDnet webcam action described above[314]—the FTC demonstrated that a company violated its own statements to consumers. This is a powerful but somewhat limited grounds for enforcement in security cases because it depends on the company having made overly strong security-related promises to the public.

The FTC has therefore also brought "unfairness" cases to attack poor security practices.[315] In unfairness cases, the FTC must show that a firm injured consumers in ways that violate public policy.[316] This is most easy in contexts with federal statutory requirements about data security, such as finance and health care. Outside of those delimited contexts, the FTC's authority is less solid. Both commentators and firms have questioned the scope of the FTC's jurisdiction in such cases.[317] Most recently, the Wyndham Hotel Group litigated that jurisdiction after the FTC alleged that Wyndham had unreasonably exposed consumer information through lax security measures.[318] Although the FTC prevailed in that challenge,[319] there is no

310. Certain information types, such as health and financial data, are subject to heightened Federal data-security requirements, but no statute sets forth general data-security measures. *See, e.g.*, Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 922 (2007) ("There is no explicit data security regulation for firms that carry out back-office and other administrative operations involving personal information.").

311. 15 U.S.C. § 45(a)(2) (2012).

312. *Id.* § 45(a)(1).

313. *E.g.*, FTC v. Accusearch Inc., 570 F.3d 1187, 1190–91 (10th Cir. 2009) (bringing an unfair-practices claim against Accusearch); *In re* GeoCities, 127 F.T.C. 94, 96 (1999) (alleging deceptive practices by GeoCities).

314. *See supra* note 304 and accompanying text.

315. *E.g.*, *In re* DSW Inc., 141 F.T.C. 117, 119–20 (2006); *In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465, 468 (2005).

316. 15 U.S.C. § 45(n).

317. *See generally* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673 (2013) (arguing that the FTC's practices may violate the fair notice doctrine). *But see* Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 812 (2011) (asserting that the FTC's privacy enforcement effort correlates with the FTC's deception and unfairness authority).

318. *See* Stegmaier & Bartnick, *supra* note 317, at 695–97.

319. *See* FTC v. Wyndham Worldwide Co., No. 13–1887(ES), 2014 WL 1349019, at *6–9 (D. N.J. Apr. 7, 2014) (holding that the FTC had authority to bring an enforcement action over data-security practices).

question that the FTC's authority in this area would be considerably strengthened by legislative action to establish data-security requirements.

As a second option, therefore, consider the possible treatment of Internet of Things security violations under state data-breach notification statutes. At the very least, one might assume that breaches of potentially sensitive—and difficult to anonymize—sensor data would be made public under such laws, just as theft of credit card data or other personal information requires public disclosure. At the moment, however, that is not the case. Forty-six states have enacted data-breach notification laws.[320] All of those cover "personal information,"[321] which is generally defined in such statutes as an individual's first and last name, plus one or more of the individual's Social Security number, driver's license number, or bank or credit card account information.[322] Thus, for the vast majority of states, a security breach that resulted in the theft of records containing users' names and associated biometric or sensor data would *not* trigger state data-breach notification requirements. A breach that only stole sensor data without users' names would also fail to trigger such laws.

---

320. ALASKA STAT. § 45.48.010 (2012); ARIZ. REV. STAT. ANN. § 44-7501 (2013); ARK. CODE ANN. § 4-110-105 (2011); CAL. CIV. CODE §§ 1798.29, 1798.82 (West Supp. 2014); COLO. REV. STAT. ANN. § 6-1-716 (West Supp. 2013); CONN. GEN. STAT. ANN. § 36a-701b (West Supp. 2014); DEL. CODE ANN. tit. 6, § 12B-102 (2013); FLA. STAT. ANN. § 817.5681 (West 2006); GA. CODE ANN. § 10-1-912 (2009); HAW. REV. STAT. ANN. §§ 487N-1 to -7 (LexisNexis 2012); IDAHO CODE ANN. § 28-51-105 (2013); 815 ILL. COMP. STAT. ANN. 530/10 to 530/12 (West 2008); IND. CODE ANN. §§ 24-4.9-3-1 to -3-2 (West Supp. 2013); IOWA CODE ANN. § 715C.2 (West Supp. 2014); KAN. STAT. ANN. § 50-7a02 (Supp. 2013); LA. REV. STAT. ANN. § 51.3074 (2012); ME. REV. STAT. ANN. tit. 10, § 1348 (Supp. 2013); MD. CODE ANN., LAB. & EMPL. §§ 14-3501 to -3508 (LexisNexis 2013); MASS. GEN. LAWS ANN. ch. 93H, §§ 1–6 (West Supp. 2014); MICH. COMP. LAWS ANN. § 445.72 (West 2011); MINN. STAT. ANN. § 325E.61 (West 2011); MISS. CODE ANN. § 75-24-29 (Supp. 2013); MO. ANN. STAT. § 407.1500 (West 2011); MONT. CODE ANN. § 30-14-1704 (2013); NEB. REV. STAT. § 87-803 (2008); NEV. REV. STAT. § 603A.220 (2013); N.H. REV. STAT. ANN. § 359-C:20 (2009); N.J. STAT. ANN. § 56:8-163 (West 2012); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2012); N.C. GEN. STAT. § 75-65 (2013); N.D. CENT. CODE §§ 51-30-02 to -30-03 (Supp. 2013); OHIO REV. CODE ANN. §§ 1347.12, 1349.19 (West Supp. 2014); OKLA. STAT. tit. 74, § 3113.1 (2011); OR. REV. STAT. § 646A.604 (2013); 73 PA. CONS. STAT. ANN. §§ 2301–2308, 2329 (West Supp. 2014); R.I. GEN. LAWS § 11-49.2-3 (Supp. 2013); S.C. CODE ANN. § 39-1-90 (Supp. 2013); TENN. CODE ANN. § 47-18-2107 (2013); TEX. BUS. & COM. CODE ANN. § 521.053 (West Supp. 2014); UTAH CODE ANN. § 13-44-202 (LexisNexis 2013); VT. STAT. ANN. tit. 9, § 2435 (Supp. 2013); VA. CODE ANN. § 18.2-186.6 (2014); *id.* § 32.1-127.1:05 (2011); WASH. REV. CODE ANN. § 19.255.010 (West 2013); *id.* § 42.56.590 (West Supp. 2014); W. VA. CODE ANN. §§ 46-2A-101 to -2A-05 (LexisNexis Supp. 2014); WIS. STAT. ANN. § 134.98 (West 2009); WYO. STAT. ANN. § 40-12-502 (2013).

321. New York's statute covers "private information." N.Y. GEN. BUS. LAW § 899-aa(b) (McKinney 2012). Vermont's covers "personally identifiable information." VT. STAT. ANN. tit. 9, § 2430(5) (Supp. 2013). The Texas statute covers "sensitive personal information." TEX. BUS. & COM. CODE ANN. § 521.002(a)(2) (West Supp. 2014).

322. *See State Data Breach Statute Form*, BAKER HOSTETLER 1 (2014), http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf, *archived at* http://perma.cc/8536-TESS (providing a general definition "based on the definition commonly used by most states").

A few anomalous jurisdictions have enacted data-breach notification laws that could be interpreted broadly to protect sensor data, but only with some creativity. The approaches of those jurisdictions can be separated into two groups. The first group includes Arkansas, California, Missouri, and Puerto Rico, which all include "medical information" in their definition of "personal information."[323] Missouri defines "medical information" to mean "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional."[324] Thus, if breached sensor data related to "mental or physical condition"—for example, personal-fitness tracking data—Missouri's statute might reach the breach. Arkansas and California define "medical information" more narrowly to mean only information "regarding the individual's medical history or medical treatment or diagnosis by a health care professional."[325] These two state statutes seem to have followed the definitions included in the Health Insurance Portability and Accountability Act (HIPAA), which defines "health information" as "any information, including genetic information, . . . that (1) [i]s created or received by a health care provider, health plan, . . . and . . . (2) [r]elates to the . . . physical or mental health or condition of an individual."[326] HIPAA's definition would most likely *not* encompass fitness- or health-related—let alone other—potentially sensitive sensor data.

The second group that differs from the norm includes Iowa, Nebraska, Texas, and Wisconsin, all of which include an individual's "unique biometric data" in their definitions of "personal information."[327] Both Nebraska and Wisconsin define "unique biometric data" to include fingerprint, voice print, and retina or iris image, as well as any "other unique physical representation."[328] This phrase might be interpreted to include at least some fitness or health-related sensor data. Texas goes further. Its statute is triggered by any breach of "[s]ensitive personal information," which includes "information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual."[329] This quite clearly would protect at least fitness-related sensor data.

---

323. ARK. CODE ANN. § 4-110-103(7)(D) (2011); CAL. CIV. CODE §§ 1798.29(e)(4), .82(e)(4) (West Supp. 2014); MO. ANN. STAT. § 407.1500(9)(e) (West 2011); P.R. LAWS ANN. tit. 10, § 4051(a)(5) (2012).

324. MO. ANN. STAT. § 407.1500(6) (West 2011).

325. ARK. CODE ANN. § 4-110-103(5) (2011); CAL. CIV. CODE § 1798.81.5(d)(2) (West Supp. 2014).

326. 45 C.F.R. § 160.103 (2013); *see* P.R. LAWS ANN. tit. 10, § 4051(a)(5) (2012) (including "[m]edical information protected by the HIPAA" within the definition of "personal information file").

327. IOWA CODE ANN. § 715C.1(11)(e) (West 2013); NEB. REV. STAT. § 87-802(5)(e) (2008); TEX. BUS. & COM. CODE ANN. § 521.002(a)(1)(C) (West Supp. 2014); WIS. STAT. ANN. § 134.98(1)(b)(5) (West 2009).

328. NEB. REV. STAT. § 87-802(5) (2008); WIS. STAT. ANN. § 134.98(1)(b)(5) (West 2009).

329. TEX. BUS. & COM. CODE ANN. § 521.002(a)(2)(B)(i) (West Supp. 2014).

Thus, in a small minority of states, health- or fitness-related sensor data—such as data produced by a Breathometer, Fitbit, Nike+ FuelBand, blood-glucose monitor, blood-pressure monitor, or other device—could arguably be protected by the state's data-breach notification law. In most, theft or breach of such data would not trigger public notification. Moreover, *none* of these state statutes would be triggered by data-security breaches into datasets containing other types of sensor data discussed in Part I. Driving-related data, for example, would nowhere be covered; location, accelerometer, or other data from a smartphone would nowhere be covered; smart grid data or data streaming out of Internet of Things home appliances would nowhere be covered. Put most simply, current data-security-breach notification laws are ill prepared to alert the public of security problems on the Internet of Things.

D. Consent

Discrimination, privacy, and security concerns about the Internet of Things underscore the new and unique ways in which connected sensor devices could harm consumer welfare. At the same time, the quick and massive growth in this market shows consumer desire for these technologies. Consumer consent offers one way to reconcile these competing realities: if consumers understand and consent to the data flows generated by their Fitbits, car monitors, smart home devices, and smartphones, perhaps there is no reason to worry. Unfortunately, consent is unlikely to provide such reassurance. Internet of Things devices complicate consent just as they complicate discrimination, privacy, and security. Moreover, consumer protection law related to privacy-policy disclosures is currently unprepared to deal with these issues.

1. The Technical Problem: Sensor Devices Confuse Notice and Choice.—Notice and choice, in other words, consumer consent, has been the dominant approach to regulating the Internet for the last decade. Regulators, legislators, and scholars have largely depended on the assumption that so long as firms provide accurate information to consumers and consumers have an opportunity to choose or reject those firms' web services, most data-related issues can be self-regulated.[330] Unfortunately, these already-stretched assumptions apply uncomfortably in the context of the consumer goods at the heart of the Internet of Things.

a. The Difficulties with Finding Internet of Things Privacy Policies.—Internet of Things devices are often small, screenless, and lacking an input

330. *See generally* Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273 (2012) (evaluating the effectiveness of the self-regulatory, notice-and-choice approach to privacy laws in the United States).

mechanism such as a keyboard or touch screen. A fitness tracker, for example, may have small lights and perhaps a tiny display, but no means to confront a user with a privacy policy or secure consent.[331] Likewise, a home electricity or water sensor, connected oven or other appliance, automobile tracking device, or other Internet of Things object will not have input and output capabilities. The basic mechanism of notice and choice—to display and seek agreement to a privacy policy—can therefore be awkward in this context because the devices in question do not facilitate consent.

This inherently complicates notice and choice for the Internet of Things. If an Internet user visits a web page, the privacy policy is available on that page. Although this does not perfectly protect consumer welfare, it at least provides a consumer with the option to review privacy- and data-related terms at the locus and time of use. Internet of Things devices, however, are currently betwixt and between. A device most likely has no means to display a privacy notice.[332] As a result, such information must be conveyed to consumers elsewhere: in the box with the device, on the manufacturer's website, or in an associated mobile application.

At the moment, Internet of Things manufacturers overwhelmingly seem to prefer to only provide privacy- and data-related information in website privacy policies. The Appendix shows the results of my survey of twenty popular Internet of Things consumer devices, including Fitbit and Nike+ Fuelband fitness trackers, the Nest Thermostat, the Breathometer, and others.[333] For many of the surveyed devices, I actually purchased the object in order to inspect the packaging and examine the consumer's experience of opening and activating the device. For others, I was able to download or secure from the manufacturer the relevant material included in the device packaging—generally the consumer user or "quick start" guides.

As indicated in the Appendix, *none* of the twenty devices included privacy- or data-related information in the box. None even referred in the packaging materials or user guides to the existence of a privacy policy on the manufacturer's website. This is reasonably surprising, given that many of these devices are for sale in traditional brick-and-mortar stores and not only through the manufacturer's website, making it possible for a consumer to purchase such a device with no notice that it is subject to a privacy policy.

Internet of Things manufacturers may currently depend on website posting of privacy policies for at least two reasons. First, they may be accustomed to including such information on a website and may not have considered that a consumer purchasing an object experiences that purchase somewhat differently than a user browsing the Internet. Second, they may believe that because Internet of Things devices generally require pairing with

---

331. *See, e.g.*, *Nike+ FuelBand SE*, *supra* note 77.

332. *See, e.g.*, *How It Works*, MIMO, http://mimobaby.com/#HowItWorks, *archived at* http://perma.cc/E6NC-WNFN.

333. *See infra* Appendix.

a smartphone app or Internet account through the manufacturer's web service, the consumer will receive adequate notice and provide adequate consent when downloading that app or activating their online account.

This belief would be unjustified. The Appendix shows that for several of the products reviewed it was extremely difficult to even locate a relevant privacy policy. Consider just one example. iHealth manufactures various health and fitness devices, including an activity and sleep tracker, a pulse oximeter, a blood-pressure wrist monitor, and a wireless body-analysis scale.[334] All of these work together through the iHealth smartphone or tablet app.[335] The privacy policy on the iHealth website, however, applies only to use of that website—not to use of iHealth products or the iHealth mobile app.[336] This suggests that iHealth assumes users will confront a second product-related privacy notice when activating the mobile app to use their products. At installation, that app presents users with a software license agreement, which states that by using the app users may upload personal information, including vital signs and other biometric data.[337] The agreement also states that "[o]ur use of Personal Data [and] VITALS [biometric data] . . . is outlined in our Privacy Policy."[338] At no point, however, is a user confronted with that product-related policy, or told where it can be located. Were a user to look on the iHealth website, he would find only the policy posted there that applies to use of the website, not to use of iHealth products. Within the mobile iHealth app, the only mention of privacy is found under the Settings function in a tab labeled "Copyright." That Copyright tab actually includes the application's Terms of Use, which again references a privacy policy that governs product use and sensor data but provides no information on where to find that policy. In short, even an interested consumer seeking privacy information about iHealth products and sensor data is led in an unending circle of confusion. This is a horrendous example of how not to provide consumers with clear notice and choice about privacy information.

The Appendix lists other examples nearly as confusing. Some policies seem to apply to both website use and sensor-device use. Other policies limit their application to website use, not sensor-device use, but provide no means to locate a device-related privacy policy. This leaves unanswered whether

334. *About Us*, iHEALTH®, http://www.ihealthlabs.com/about-us/, *archived at* http://perma.cc/5KY5-U953.

335. *Id.*

336. *See Privacy Policy*, iHEALTH®, http://www.ihealthlabs.com/about-us/privacy-policy/, *archived at* http://perma.cc/47CK-9XJP (setting forth the privacy policy governing information collected from visitors, users, and customers of iHealth's website but not discussing privacy policies regarding data gleaned from iHealth devices).

337. *See* iHEALTH, TERMS AND CONDITIONS: SOFTWARE END USER LICENSE AGREEMENT (on file with author) (stating that by using the iHealth app services, users may upload personal data information such as name, e-mail, height, weight, age, and "Vitals" information contained in the monitoring hardware purchased from iHealth).

338. *Id.*

any privacy-related policy applies to the data generated by these devices.[339] In still other cases, two privacy policies vie for users' attention: one for website use, one for sensor device use. In some ways this is a better approach, because it provides clear notice that the sensor device comes with a unique set of data-related and privacy issues. At the same time, this doubles the cognitive and attentional load on consumers, who already fail to read even one privacy policy. This approach may also create confusion if consumers see the website policy and fail to realize that a second policy exists related to their sensor data.

In addition to the problem of *finding* a relevant privacy policy, the Appendix shows that even when one locates a policy that applies to use of these products and the sensor data they generate, many current Internet of Things privacy policies provide little real guidance to consumers. My review of these twenty products and their privacy policies reveals two major problems.

b. The Ambiguity of Current Internet of Things Privacy-Policy Language.—First, these policies are often confusing about whether sensor or biometric data count as "personal information" and thus unclear about how such data can be shared with or sold to third parties.[340] Some of these policies define "personal information" (or "personally identifiable information") in a very traditional manner, as including only name, address, e-mail address, or telephone number.[341] For such policies, sensor data would not be given the heightened protections afforded to personally identifiable information.

Other policies are significantly less clear. Some include language that might be interpreted to include sensor data. Breathometer's privacy policy, for example, defines "personal information" as "information that directly identifies you, or that can directly identify you, such as your name, shipping and/or billing address, e-mail address, phone number, and/or credit card information."[342] Although this would generally suggest that sensor data are not included, a computer scientist or regulator that understands the problem of re-identification might interpret this to mean that test results *were* included as personal information. The Breathometer privacy policy adds to the confusion. In a section titled "Personal Information We Affirmatively

339. In at least one case, the website privacy policy stated that a second sensor device policy existed, but that second policy was only accessible through a separate website. *Privacy Policy*, PROPELLER HEALTH, http://propellerhealth.com/privacy/, *archived at* http://perma.cc/6SBE-BJE5; *Propeller User Agreement*, PROPELLER, https://my.propellerhealth.com/terms-of-service, *archived at* http://perma.cc/697K-TQVU.

340. This problem extends beyond Internet of Things policies. *See* Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 458 (2013) (providing an empirical review of terms of service and privacy policies for cloud computing services and concluding that such policies rarely provide much detail on firms' obligations to consumers).

341. *See infra* Appendix.

342. *Privacy Policy*, BREATHOMETER™, *supra* note 17.

Collect From You," the policy states that "[u]ser-generated content (such as BAC Test results) may include Personal Information."[343] This further confuses whether the company will treat sensor readings from a Breathometer as personal information under the policy.

Similarly, the Nest Thermostat's privacy policy defines "Personally Identifiable Information" as "data that can be reasonably linked to a specific individual or household."[344] Given the threat of re-identification of Internet of Things sensor data, it is entirely unclear whether the policy's drafters consider Nest Thermostat data to be personally identifiable. This same issue arises in the Belkin WeMo home automation system privacy policy. That policy defines personal information as "any information that can be used to identify you."[345] One might therefore believe this to include sensor data if such data is easily re-identified. The policy then goes on, however, to state that "Non-Personal Information" includes "usage data relating to . . . Belkin Products."[346] In other words, the policy creates conflict between its definition of "personal information" and "non-personal information."

This definitional wrangling matters. Most privacy policies permit manufacturers to share or sell non-personal information far more broadly than personal information. The LifeBEAM Helmet privacy policy, for example, allows non-personal information to be collected, used, transferred, and disclosed for any purpose, but states that "LifeBEAM does not disclose personally-identifying information."[347] In addition, certain other terms in these privacy policies apply only to personal information. For example, the Breathometer policy contractually provides for user notification in the event of a security breach that compromises personal information.[348] Because the policy leaves unclear whether sensor data are personal information, it is unclear whether a user should expect notification in the event that sensor data were breached. Similarly, the Mimo Baby Monitor policy gives broad access, correction, and deletion rights to users for "Personal Information" but makes no mention of how such rights apply to other information.[349]

In short, these Internet of Things privacy policies are often quite unclear about whether collected sensor data count as "personal information"—and therefore ambiguous as to what rights and obligations apply to such data.

---

343. *Id.*

344. *Privacy Statement*, NEST, https://nest.com/legal/privacy-statement/, *archived at* http://perma.cc/V5JC-GGT4.

345. *Belkin Privacy Policy*, BELKIN, http://www.belkin.com/us/privacypolicy/, *archived at* http://perma.cc/8VFG-T3CF.

346. *Id.*

347. *LifeBEAM Privacy Policy*, LIFEBEAM, http://www.life-beam.com/privacy, *archived at* http://perma.cc/6ET2-J284.

348. *See Privacy Policy*, BREATHOMETER™, *supra* note 17.

349. *Privacy Policy*, MIMO, http://mimobaby.com/legal/#PrivacyPolicy, *archived at* http://perma.cc/64RN-6K7D.

c. The Glaring Omissions from Internet of Things Privacy Policies.— Second, the privacy policies for these devices often do not address several important issues relevant to consumers. For example, privacy policies for consumer sensor devices often do not mention ownership of sensor data. Of the twenty products covered by the Appendix, only four discussed data ownership explicitly. Of those that did clarify ownership of sensor data, three indicated that the *manufacturer*, not the consumer, owned the sensor data in question.[350] The BodyMedia Armband's policy, for example, states that "[a]ll data collected including, but not limited to, food-logs, weight, body-fat-percentage, sensor-data, time recordings, and physiological data . . . are and shall remain the sole and exclusive property of BodyMedia."[351] The previous version of the Basis Sports Watch policy similarly stated that "[a]ll Biometric Data shall remain the sole and exclusive property of BASIS Science, Inc."[352] It is only some consolation that at least ownership is clear in these few cases.

Similarly, these policies often do not specify exactly what data the device collects or which types of sensors the device employs. Of the twenty products reviewed, only three provided clear information on exactly what sensors the product included or what sensor data the product collected.[353] A few more provided some information on data collected without complete detail. For example, the privacy policy relevant to the Automatic Link automobile monitor describes that the device collects location information, information on "how you drive," error codes from the car's computer, and information from both the car's sensors and the device's sensors.[354] The policy does not give detail about what car or device sensors are used or what exactly the device records about "how you drive." Moreover, the Appendix shows that many of these Internet of Things privacy policies provided *no* information on what sensor data their device generated.

These policies are likewise inconsistent in the access, modification, and deletion rights they give consumers. Most of the twenty policies I reviewed said nothing about such rights. None provided an easy mechanism for

350. These four devices are the BodyMedia Armband, iHealth Blood Pressure Monitor, Basis Peak sports watch, and Muse headband; the Muse headband is the only device for which the policy indicated the user owned the biometric or sensor data. *See infra* Appendix. Basis recently updated the privacy policy on September 29, 2014, removing the data-ownership language. *See Basis Privacy Policy*, BASIS, http://www.mybasis.com/legal/privacy/, *archived at* http://perma.cc/5GYH-Q3JP.

351. *Privacy Policy*, BODYMEDIA®, http://www.bodymedia.com/Support-Help/Policies/Privacy-Policy, *archived at* http://perma.cc/M8HF-5EWV.

352. The new version of the privacy policy removed that ownership language; the only ownership language in the new policy states that the user "will be notified via email of any . . . change in ownership or control of personal information" arising from a "business transition" undertaken by Basis. *Basis Privacy Policy*, *supra* note 350.

353. These devices are the Basis Peak sports watch, Mimo Baby Monitor, and Nest Thermostat or Smoke Detector. *See infra* Appendix.

354. *Legal Information: Privacy Policy*, AUTOMATIC™, http://www.automatic.com/legal/#privacy, *archived at* http://perma.cc/R6BR-23PA.

exportation of raw sensor data. And many were quite confusing about what access, modification, and deletion rights a consumer had. These privacy policies sometimes gave users such rights for personal information but not for other (non-personal) information.[355] As discussed, it is often unclear whether sensor or biometric data count as "personal information," and therefore unclear whether users have modification and deletion rights vis-à-vis those data.[356]

Finally, none of these policies explained how much sensor data were processed on the device itself versus transmitted to and processed on the company's servers remotely. Only three detailed whether encryption techniques were used to protect sensor-gathered data or what techniques were specifically employed.[357] None detailed the security measures built into the device itself to prevent security breach.

In short, these policies seem to have been shaped by the needs and expectations relevant to the normal Internet, not the Internet of Things. Not surprisingly, at the dawn of the Internet of Things, there may not yet have been much real consideration of the special issues that Internet of Things privacy policies should address.[358]

2. The Legal Problem: Consumer Protection Law Is Unprepared.—As discussed above, the FTC's mandate is to police deceptive and unfair trade practices.[359] In the privacy-policy context, this includes taking action against firms that violate their posted privacy policies,[360] as well as providing soft guidance to firms on what constitutes adequate notice in a privacy policy.[361]

---

355. *See supra* note 349 and accompanying text.

356. *See supra* subsection II(D)(1)(b).

357. The Basis Peak sports watch and Mimo Baby Monitor privacy policies state that biometric data are not encrypted; the Nest Thermostat states that data are encrypted. *See infra* Appendix.

358. There has been some academic work on Internet of Things privacy policies, but nothing in mainstream legal scholarship. *See, e.g.*, R.I. Singh et al., *Evaluating the Readability of Privacy Policies in Mobile Environments*, 3 INT'L J. MOBILE HUM. COMPUTER INTERACTION 55, 55–56 (2011) (exploring the differences between viewing privacy policies on a desktop and on a mobile device); Sebastian Speiser et al., *Web Technologies and Privacy Policies for the Smart Grid*, *in* IECON 2013: PROCEEDINGS OF THE 39TH ANNUAL CONFERENCE OF THE IEEE INDUSTRIAL ELECTRONICS SOCIETY 4809, 4811–12 (2013) (examining privacy policies and proposing a new architecture for "privacy aware" policy frameworks in the context of smart grids).

359. *See supra* notes 310–14 and accompanying text.

360. *E.g.*, *In re* GeoCities, 127 F.T.C. 94, 122–32 (1999) (ordering various remedial actions to be taken by GeoCities based on allegations that GeoCities had misrepresented its privacy policy).

361. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 27–28 (2000), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf, *archived at* http://perma.cc/4YEU-TPJX (recommending prominently displayed links to privacy policies on a website's home page and anywhere that personal information is collected). Various commentators have called for more substantive or legislative guidance on what terms should be included in online privacy policies. *See* Kesan et al., *supra* note 340, at 460 ("We recommend a new legal regime that would emphasize empowering

Although the FTC held its first public workshop on the Internet of Things in November 2013,[362] it has yet to release guidelines or policy recommendations specifically related to privacy policies on the Internet of Things. Manufacturers therefore have no tailored guidance from the FTC about what constitutes adequate notice in Internet of Things privacy policies.

California's Office of Privacy Protection has taken the lead among states in setting out recommended practices on privacy policies.[363] California's Online Privacy Protection Act (COPPA)[364] requires a firm operating a "commercial Web site or online service" that collects personally identifiable information to "conspicuously post" a privacy policy, either on the website or, in the case of an "online service," through "any other reasonably accessible means of making the privacy policy available for consumers of the online service."[365] The policy must identify the categories of PII collected and types of third parties with whom the company shares information.[366] If the firm provides consumers a mechanism to access or correct PII, the policy must explain that process.[367] In 2008, the California Office of Privacy Protection issued nonbinding guidelines for compliance with these requirements. These guidelines urge firms to include in their privacy policies information on how they collect personal information, what kinds of personal information they collect, how they use and share such information with others, and how they protect data security.[368] In addition, California has recently promulgated guidelines for how best to adapt privacy policies to the smaller screens of mobile phones.[369]

Internet of Things firms clearly trigger COPPA's requirement to have a privacy policy, either because they maintain a website or because they operate an "online service." They must thus disclose the types of PII collected and the categories of third parties with whom they share that PII.[370] This is precisely what we see in existing policies, as discussed above.[371] Because neither the FTC nor California—nor any other relevant legislative or regulatory actor—has set forth requirements specifically applicable to the Internet of Things context, firms are undoubtedly using these baseline website requirements as a minimal safe harbor. They are promulgating

---

consumers by setting a baseline of protection to ensure that a consumer has control over her own data.").

362. *See supra* note 50 and accompanying text.

363. CA. OFFICE OF PRIVACY PROT., RECOMMENDED PRACTICES ON CALIFORNIA INFORMATION-SHARING DISCLOSURES AND PRIVACY POLICY STATEMENTS (2008).

364. CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2008).

365. *Id.* §§ 22575(a), 22577(b)(1), (5).

366. *Id.* § 22575(b)(1).

367. *Id.* § 22575(b)(2).

368. CA. OFFICE OF PRIVACY PROT., *supra* note 363, at 12–14.

369. CA. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM, at i, 9–13 (2013).

370. *See supra* note 366 and accompanying text.

371. *See supra* subsection II(D)(1)(b).

privacy policies that meet legal requirements created for the Internet, not the Internet of Things.

In short, consumer protection law is essentially unprepared for the Internet of Things. Clearly, firms cannot post deceptive privacy policies for Internet of Things devices, but that is relatively little comfort. Neither the FTC nor California has provided substantive guidance on information disclosure for Internet of Things devices. California's privacy policy law has not been revised since 2008, long before the Internet of Things began to take shape. Not surprisingly, then, notice and choice is off to a rocky start in the Internet of Things context.

III. Four (Messy & Imperfect) First Steps

Let us review the argument to this point. The Internet of Things is developing rapidly as connected sensor-based consumer devices proliferate. Millions of health and fitness, automotive, home, employment, and smartphone devices are now in use, collecting data on consumers' behaviors. These sensor-based data are so granular and high quality that they permit often profound and unexpected inferences about personality, character, preferences, and even intentions. The Internet of Things thus gives rise to difficult discrimination problems, both because seemingly innocuous sensor data might be used as proxies in illegal racial, age, or gender discrimination and because highly tailored economic sorting is itself controversial. In addition, Internet of Things data are difficult to anonymize and secure, creating privacy problems. Finally, notice and choice is an ill-fitting solution to these problems, both because Internet of Things devices may not provide consumers with inherent notice that data rights are implicated in their use and because sensor-device firms seem stuck in a notice paradigm designed for websites rather than connected consumer goods. Currently, discrimination, privacy, security, and consumer welfare law are all unprepared to handle the legal implications of these new technologies.

This Part does not propose a grand solution to these problems. I do not call for a new federal statute or urge the creation of a new regulatory agency. Such solutions would be elegant but implausible, at least at the moment. Scholars have argued for such comprehensive privacy reforms for the last decade,[372] and Congress has ignored them. The futility of such large-scale projects thus leads me to suggest smaller and more eclectic first steps that have some chance of actual effect.

I do not attempt to impose a theoretically consistent approach on these four first steps. One might, for example, demand procedural due process for

372. *See, e.g.*, Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 (proposing a "Model Regime" to correct legislative inadequacies in consumer privacy protections).

consumers[373] or argue for state (as opposed to federal) or federal (as opposed to state) intervention. I walk a different line, making use of both procedural and more substantive solutions, as well as both federal and state reforms. My purpose is not to propose a course that is perfectly consistent, but instead one that can be realistic and pragmatic. I therefore suggest four messy and imperfect first steps toward regulating the Internet of Things: (1) broadening existing use constraints—such as some state law on automobile EDRs—to dampen discrimination; (2) redefining "personally identifiable information" to include biometric and other forms of sensor data; (3) protecting security by expanding state data-breach notification laws to include security violations related to the Internet of Things; and (4) improving consent by providing guidance on how notice and choice should function in the context of the Internet of Things.

My goal is to provoke regulatory and scholarly discussion, as well as to provide initial guidance to corporate counsel advising Internet of Things firms at this early stage. In this, I borrow from recent work by Kenneth Bamberger and Dierdre Mulligan, who have argued persuasively that chief privacy officers and corporate counsel need such guidance on how to uphold consumer expectations.[374] If privacy regulation focuses exclusively on procedural mechanisms for ensuring notice and choice, corporate decision makers will likewise focus on such procedural moves. They will tweak their privacy policies, enlarge their fonts, and add more bells and whistles to such policies to try to satisfy regulators. But such hoop jumping may have little real impact on consumer welfare. Providing substantive guidance to corporations, however, may lead corporate decision makers down a different path. If legislators, regulators, and the privacy community make clear their substantive expectations for the Internet of Things, corporations will likely use such norms as guidance for what consumers expect and demand. This is the "privacy-protective power of substantive consumer expectations overlaid onto procedural protections."[375]

My goal in this Part is to suggest ways in which regulators, legislators, and privacy advocates can begin to provide such substantive guidance to the firms creating the Internet of Things. The Part concludes with a public choice argument for urgency—suggesting that we can and must move quickly to set

373. *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 126–27 (2014) (arguing that opportunities for consumers to air their privacy grievances before a "neutral data arbiter" would comport with core values of procedural due process).

374. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 298 (2011) ("[D]ecisions at the corporate level might provide the best way to avoid privacy harms. . . . [P]roviding a substantive metric to guide such systemic decisions recognizes the fact that the values embedded in technology systems and practices shape the range of privacy-protective choices individuals can and do make . . . ." (footnote omitted)).

375. *Id.* at 300.

guidelines and ground rules before economic interests in the Internet of Things ecosystem become overly entrenched and immovable.

A. A Regulatory Blueprint for the Internet of Things

1. Dampening Discrimination with Use Constraints.—Use constraints—or "don't use" rules[376]—are common across the law. Fifth Amendment jurisprudence prohibits a jury from drawing negative inferences from a defendant's failure to testify;[377] the FCRA bars consumer reporting agencies from including bankruptcies more than ten years old in consumer credit reports;[378] and the GINA bars the use of genetic information by health insurers.[379] Such rules

> rest on a social judgment that even if transacting parties both wish to reveal and use a particular piece of information, its use should be forbidden because of some social harm, such as discriminating against those with genetic disorders, that is greater than the social benefits, such as the allocative and contractual efficiency created by allowing freedom of contract.[380]

As a first regulatory step, we should constrain certain uses of Internet of Things data if such uses threaten consumer expectations. This approach is substantive rather than procedural, and sectoral rather than comprehensive.[381] The advantages of such an approach include that one can tailor such constraints to each particular context and prioritize those contexts that present the most risk of consumer harm. In addition, one can sometimes mobilize legislators and regulators that become concerned about discriminatory uses of information in a particular context and galvanized about that type of use, but who might not adopt more widespread, systemic reforms.

Consider two broad categories of—and justifications for—use constraints: constraints on cross-context use of data and constraints on forced data revelation even within a given context.

---

376. *See* Peppet, *supra* note 48, at 1199 (discussing how "don't use" rules constrain the decision-making process by restricting information).

377. *E.g.*, Mitchell v. United States, 526 U.S. 314, 328 (1999) (holding that the rule against negative inferences applies equally to sentencing hearings as to criminal trials); Carter v. Kentucky, 450 U.S. 288, 305 (1981) (reaffirming precedent requiring judges to charge juries with "no-inference" instructions when requested by a party asserting Fifth Amendment privileges in a criminal case).

378. *See* 15 U.S.C. § 1681c(a)(1) (2012).

379. *See* 29 U.S.C. § 1182(a)(1) (2012) ("[A] health insurance issuer . . . may not establish rules for eligibility . . . based on . . . [g]enetic information.").

380. Peppet, *supra* note 48, at 1200.

381. In contrast, for example, consider a recent proposal by Tene and Polonetsky calling for increased decisional transparency—requiring organizations that *use* data to disclose how they do so and for what purposes. *See* Tene & Polonetsky, *supra* note 19, ¶ 86 ("[W]e propose that organizations reveal not only the existence of their databases but also the *criteria* used in their decision-making processes . . . .").

a. Cross-Context Use Constraints.—First, borrowing from Helen Nissenbaum's work on the importance of restraining cross-context data flows to protect consumer privacy,[382] privacy advocates should focus on keeping Internet of Things data use from violating contextual boundaries. Some choices will be easy. Racial, gender, age, and other forms of already illegal discrimination are likely to generate immediate and sympathetic responses. If an employer, insurer, or other economic actor were to begin using Internet of Things data as a proxy for race or other protected characteristics, legislators and regulators are sure to react.

Beyond racial and other forms of illegal discrimination, there is some reason for optimism, however, that use constraints are possible to dampen economic discrimination based on cross-context use of Internet of Things data. State legislatures—far more so than Congress—have enacted a variety of use constraints that protect consumers' information. For example, although relatively little attention has been paid in the legal literature to the use of diverse sources of information in credit scoring,[383] there has been some debate over whether lenders should be permitted to access social media—Facebook, LinkedIn, Twitter—to factor one's social context into credit determinations.[384] Similarly, controversy erupted a few years ago when it was publicized that auto insurers were factoring FICO credit scores into auto insurance rate setting.[385] Consumer groups protested that this cross-context use of information was unfair and opaque to consumers.[386] Finally, several states, including California, Connecticut, Hawaii, Illinois, Maryland, Oregon, and Washington, have passed laws limiting employers' consideration of credit reports,[387] even though research has shown that credit scores

382. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 2–4 (2010) (constructing a privacy framework centered on "contextual integrity" that seeks to incorporate constraints from various sources, such as social norms, policy, law, and technical design).

383. *See* Cullerton, *supra* note 257, at 808 ("Although much scholarly attention has been paid to the privacy implications of online data mining and aggregation, . . . for use in targeted behavioral advertising, relatively little attention has been focused on the adoption of these techniques by lenders." (footnote omitted)). *See generally* Lea Shepard, *Toward a Stronger Financial History Antidiscrimination Norm*, 53 B.C. L. REV. 1695, 1700–05 (2012) (detailing the information included in consumer reports and credit reports).

384. *See, e.g.*, *Stat Oil: Lenders Are Turning to Social Media to Assess Borrowers*, ECONOMIST, Feb. 9, 2013, http://www.economist.com/news/finance-and-economics/21571468-lenders-are-turning-social-media-assess-borrowers-stat-oil, *archived at* http://perma.cc/KE7J-3LF4 (warning about potential concerns with considering social media in lending decisions).

385. *See* Herb Weisbaum, *Insurance Firms Blasted for Credit Score Rules*, NBCNEWS (Jan. 27, 2010, 5:02 PM), http://www.nbcnews.com/id/35103647/ns/business-consumer_news/t/insurance-firms-blasted-credit-score-rules/#.VAzDthbfXww, *archived at* http://perma.cc/3ZTL-FPUK (providing an overview of how credit scores are used in the insurance industry and describing the backlash to that practice).

386. *Id.*

387. CAL. LAB. CODE § 1024.5(a) (West Supp. 2014); CONN. GEN. STAT. ANN. § 31-51tt (West Supp. 2014); HAW. REV. STAT. ANN. § 378-2(8) (2010); 820 ILL. COMP. STAT. ANN. 70/10 (West

correlate with traits such as impulsivity, self-control or impatience, and trustworthiness.[388] Such traits are relevant to employers—but inferences drawn from one context can be disturbing if used in another.[389]

Similarly, state legislators may be galvanized to take action on the use of data emerging from the many Internet of Things devices that track and measure two of our most privacy-sensitive contexts: the body and the home. Although fitness, health, appliance use, and home habit data may be economically valuable in employment, insurance, and credit decisions, it is also likely that the public will react strongly to discrimination based on such sensitive information.

Advocates, regulators, and legislators might therefore consider these two domains as worthy candidates for cross-context use constraints. First, the explosion of fitness and health monitoring devices is no doubt highly beneficial to public health and worth encouraging. At the same time, data from these Internet of Things devices should not be usable by insurers to set health, life, car, or other premiums. Nor should these data migrate into employment decisions, credit decisions, housing decisions, or other areas of public life. To aid the development of the Internet of Things—and reap the potential public-health benefits these devices can create—we should reassure the public that their health data will not be used to draw unexpected inferences or incorporated into economic decision making. A woman tracking her fertility should not fear that a potential employer could access such information and deny her employment; a senior employee monitoring his fitness regime should not worry that his irregular heart rate or lack of exercise will lead to demotion or termination; a potential homeowner seeking a new mortgage should not be concerned that in order to apply for a loan she will have to reveal her fitness data to a bank as an indicator of character, diligence, or personality.

Second, Internet of Things devices in the home should be similarly protected. As indicated, it is relatively easy to draw powerful inferences about a person's character from the intimate details of her home life.[390] Whether and how often a person comes home late at night, how regularly she cooks for herself, how often she uses her vacuum to clean her home, with what frequency she leaves her oven on or her garage door open as she leaves the house, whether she turns on her security system at night—all of these

---

Supp. 2014); MD. CODE ANN., LAB. & EMPL. § 3-711(b) (LexisNexis Supp. 2013); OR. REV. STAT. § 659A.320 (2013); WASH. REV. CODE ANN. § 19.182.020 (West 2013).

388. Shweta Arya et al., *Anatomy of the Credit Score*, 95 J. ECON. BEHAV. & ORG. 175, 176–77 (2013).

389. *See* Ruth Desmond, Comment, *Consumer Credit Reports and Privacy in the Employment Context: The Fair Credit Reporting Act and the Equal Employment for All Act*, 44 U.S.F. L. REV. 907, 911–12 (2010) (lamenting that the availability of credit reports, which often give incomplete and out-of-context information, allows employers to "draw potentially misleading conclusions about a person's history and behavior").

390. *See supra* subpart I(C).

intimate facts could be the basis for unending inference. Currently there is little to prevent a lender, employer, insurer, or other economic actor from seeking or demanding access to such information. Given the personal nature of such data, however, this seems like a ripe area for cross-context use constraints to prevent such invasive practices.

Some will undoubtedly object to this call for cross-context use constraints, arguing that the economic benefits of using such data to tailor economic decisions outweigh any social costs. I disagree. Just because everything may reveal everything on the Internet of Things, it does not follow that all uses of all data necessarily benefit social welfare.[391] If any contexts demand respect and autonomy, the body and the home seem likely candidates. Moreover, for the Internet of Things to flourish, consumers must be reassured that overly aggressive, cross-context uses of data will be controlled. Early research suggests, for example, that consumers have been slow to adopt car-insurance telematics devices out of fear that their driving data will leak into other contexts such as employment.[392] Research on personal fitness monitors reveals similar fears.[393] Reasonable constraints on cross-context data use will likely facilitate, not inhibit, the development of the Internet of Things.

b. Constraints on Forced Disclosure Even Within a Given Context.— As a second category, legislators should consider use constraints *within* a given context to prevent forced disclosure of sensitive Internet of Things data. Whereas cross-context use constraints derive their legitimacy from privacy theory that shows that context-violating data use threatens consumer expectations and welfare, this second type of within-context use constraints is grounded in the assumption that consumers should not be forced to reveal certain information through economic or other pressure.

To understand this second type of use constraint and how it differs from cross-context constraints, return to the example of automobile EDRs. Privacy advocacy groups have argued for use constraints in this context. The Electronic Privacy Information Center (EPIC), for example, has urged the NHTSA to limit use of EDR data.[394] In particular, EPIC has argued that insurers should be forbidden from requiring access to EDR data as a

391. *See supra* notes 249–50 and accompanying text.

392. *See* Johannes Paefgen et al., *Resolving the Misalignment Between Consumer Privacy Concerns and Ubiquitous IS Design: The Case of Usage-Based Insurance*, *in* ICIS 2012: PROCEEDINGS OF THE 33RD INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS 1, 2 (2012) ("[T]he slow diffusion rate of [usage-based motor insurance] has been attributed to [privacy concerns] among potential customers . . . .").

393. *See infra* section III(A)(4).

394. Comment of the Elec. Privacy Info. Ctr. et al., to the Nat'l Highway Traffic Safety Admin., Docket No. NHTSA-2012-0177, at 2 (Feb. 11, 2013), *available at* http://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf, *archived at* http://perma.cc/H6EK-BAKY (responding to Federal Motor Vehicle Saftey Standards; Event Data Recorders, 49 Fed. Reg. 74,144 (Dec. 13, 2012)).

condition of insurability, using EDR data for premium assessment, or conditioning the payment of a claim on the use of such data.[395] Likewise, several states have passed laws limiting EDR data use.[396] Four states currently forbid insurance companies from requiring that an insured consent to future disclosure of EDR data or from requiring access to EDR data as a condition of settling an insurance claim.[397] One state—Virginia—also forbids an insurer from adjusting rates solely based on an insured's refusal to provide EDR data.[398]

These statutes illustrate how use constraints can substantively limit data use *within* a given context. They enact the judgment that insurers should not use economic pressure to force consumers to reveal automobile sensor data. Other states should consider enacting these restrictions on EDR data.

In addition, however, state legislatures should broaden these statutes. Most of these state statutes currently would not cover the data generated by consumer driving and automobile monitors, such as the Automatic Link sensor device described in Part I.[399] Several states, including Arkansas, California, Colorado, Nevada, New Hampshire, and Texas, limit their EDR statutes to factory- or manufacturer-installed data recorders.[400] These statutes thus do not apply to a consumer-installed after-market device. Other states, including Connecticut, Oregon, and Utah, limit their statutory protections only to devices that record vehicle data just prior to or after a crash event.[401] Again, this would—somewhat ironically—exclude Internet of Things

395. *Id.* at 12.

396. Fifteen states have passed laws related to EDR data. ARK. CODE ANN. § 23-112-107 (2014); CAL. VEH. CODE § 9951 (West Supp. 2014); COLO. REV. STAT. ANN. § 12-6-402 (2010); CONN. GEN. STAT. ANN. § 14-164aa (West Supp. 2014); ME. REV. STAT. ANN. tit. 29-A, §§ 1971–1973 (Supp. 2013); NEV. REV. STAT. § 484D.485 (2013); N.H. REV. STAT. ANN. § 357-G:1 (2009); N.Y. VEH. & TRAF. LAW § 416-b (McKinney 2011); N.D. CENT. CODE § 51-07-28 (2007); OR. REV. STAT. §§ 105.925, .928, .932, .935, .938, .942, .945 (2013); TEX. TRANSP. CODE ANN. § 547.615(c), (d) (West 2011); UTAH CODE ANN. § 41-1a-1503 (LexisNexis Supp. 2013); VA. CODE ANN. §§ 38.2-2212(C.1)(s), -2213.1, 46.2-1088.6, -1532.2 (2007); WASH. REV. CODE ANN. § 46.35.030 (West 2012); H.R. 56, 147th Gen. Assemb., Reg. Sess. (Del. 2014); *see Privacy of Data from Event Data Recorders: State Statutes*, *supra* note 27 (elaborating and distinguishing the substance of these states' statutes).

397. ARK. CODE ANN. § 23-112-107(e)(3)–(4) (2014); N.D. CENT. CODE § 51-07-28(6) (2007); OR. REV. STAT. § 105.932 (2013); VA. CODE ANN. § 38.2-2212(C.1)(s) (2007).

398. VA. CODE ANN. § 38.2-2213.1 (2007).

399. *See supra* notes 113–18 and accompanying text.

400. ARK. CODE ANN. § 23-112-107(a)(2) (2014); CAL. VEH. CODE § 9951(b) (West Supp. 2014); COLO. REV. STAT. ANN. § 12-6-401(2) (2010); NEV. REV. STAT. § 484D.485(6) (2013); N.H. REV. STAT. ANN. § 357-G:1(II) (2009); TEX. TRANSP. CODE ANN. § 547.615(a)(2) (West 2011).

401. CONN. GEN. STAT. ANN. § 14-164aa(a)(1) (West Supp. 2014); OR. REV. STAT. § 105.925(1) (2013) (adopting the definition in 49 C.F.R. § 563.5(b) as of January 1, 2008); UTAH CODE ANN. § 41-1a-1502(2) (LexisNexis Supp. 2013) (adopting the definition in 49 C.F.R. § 563.5(b) as of May 14, 2013); *see also* 49 C.F.R. § 563.5(b) (2007) (defining EDR as a device recording "during the time period just prior to a crash event . . . or during a crash event"); *id.* § 563.5(b) (2013) (same).

devices such as the Automatic Link that record far *more* information around-the-clock.

Two states—Virginia and Washington—have enacted broader EDR statutes that would protect Internet of Things data from compelled use by an insurer. Virginia and Washington define a "recording device" broadly as "an electronic system . . . that primarily . . . preserves or records . . . data collected by sensors . . . within the vehicle."[402] If other states adopt new EDR statutes—or states with existing but limited EDR statutes consider revision—they should extend their statutory protections to data collected by after-market consumer Internet of Things devices, not merely manufacturer-installed crash-related EDRs. Doing so will ensure that consumers can experiment with the Internet of Things without fear that an insurance company will compel revelation of their data.

In addition, however, states considering new or revised EDR statutes should take seriously the threat that everything reveals everything. Use constraints could restrict the use of automobile and driving data for employment, credit, and housing decisions, as well as for insurance decisions outside of the car-insurance context (e.g., health or life insurance), when the decision in question does not directly relate to driving. Thus, if an employer wanted access to driving data from its fleet of vehicles in order to improve fleet efficiency or oversee its drivers' safety, such directly related uses should be permitted. But if an employer sought access to an employee's personal Internet of Things data to make hiring or other employment decisions, a state EDR statute should prevent forced revelation of such information.

By this point it might seem overly detailed to consider this one example—automobile EDR data—so carefully. I predict, however, that the control of Internet of Things data will have to happen in this fine-grained way. Each context, device, or type of data will need to be considered. The opportunities for and risks of discrimination based on that data will have to be weighed. And legislators will have to decide whether allowing such sensor data to leak into unexpected and sensitive contexts harms consumer welfare.

Various contexts are ripe for consideration. One can easily imagine health and life insurers demanding or seeking access to fitness and health sensor data, or home insurers demanding access to home-monitoring system data. As such data become more detailed, sensitive, and revealing, states might consider prohibiting insurers from conditioning coverage on their revelation. The Nest Protect, for example, not only alerts a consumer about smoke alarms, but also contains motion sensors that track how and when

402. VA. CODE ANN. § 46.2-1088.6(A)(6) (2007); WASH. REV. CODE ANN. § 46.35.010(2) (West 2012).

users inhabit different parts of their homes.[403] Although such information might be useful to a home insurer to investigate a fire or casualty claim, it seems invasive to permit insurers to demand such detailed information as a condition of insurance.

Similarly, legislators might consider within-context constraints on employers who demand disclosure of personal Internet of Things data streams. The Lumo Back posture sensor, for example, is a strap that one wears around one's midsection.[404] It constantly monitors one's posture and can aid in recovery from back injuries.[405] One can imagine an employer becoming quite interested in such data if it were prosecuting a worker's compensation claim or investigating an employee's work habits in a factory or warehouse. Forcing disclosure of such information, however, will likely kill consumer interest in such devices over time. Reasonable within-context use constraints might dampen these problems.

Some will no doubt object that within-context use constraints are overly paternalistic and will prevent certain consumers from making use of their Internet of Things data to distinguish themselves in the market as good, trustworthy, diligent economic actors. I have argued elsewhere that forced disclosure is and will likely become increasingly problematic as biometric and other sensors proliferate.[406] There is no reason to repeat that long and somewhat complex argument here. For now, I will simply conclude that Internet of Things devices are likely to create a variety of within-context forced-disclosure examples that may provoke legislative reaction.

Of course, in the end my judgment is irrelevant: legislators—particularly state legislators—will have to weigh consumer welfare and determine whether such use constraints seem justified. At the moment these issues of discrimination are not even on the regulatory radar screen. Hopefully this proposal to employ use constraints to dampen discrimination based on the Internet of Things will begin that conversation.

2. Protecting Privacy by Redefining Personally Identifiable Information in This Context.—A second plausible initial step is to focus attention on how the terms "personal information" or "personally identifiable information" are used in relation to Internet of Things data. As indicated in Part II, both academic commentators and the FTC have already begun to move from a binary definition—where information is or is not PII—to a more nuanced approach in which regulation becomes more strict as information

403. *See Nest Support*, NEST, https://support.nest.com/article/Learn-more-about-the-Nest-Protect-sensors, *archived at* http://perma.cc/JT6H-772W (describing the Nest Protect's ultrasonic and occupancy sensors that detect movement and proximity).

404. *Lumo Back*, *supra* note 84.

405. *The Science of LUMOback*, LUMO, http://www.lumoback.com/learn/the-science-of-lumo back, *archived at* http://perma.cc/NUK6-JDPY.

406. *See* Peppet, *supra* note 48, at 1159 ("[I]n a signaling economy, the stigma of nondisclosure may be worse than the potential discriminatory consequences of full disclosure.").

becomes more *likely* to identify or be identified with an individual.[407] Neither scholars nor regulators, however, have focused on the particular issues for PII raised by the Internet of Things.[408] This has left the door open for Internet of Things firms to define "personal information" and "personally identifiable information" in a variety of ways in privacy policies and terms of use, as indicated by the privacy-policy survey discussed in Part II.[409]

As a first step, regulators should issue guidance to Internet of Things firms about how to define and treat personally identifiable information in their privacy policies, on their websites generally, and in their security practices. Part II asserted that sensor data are particularly difficult to anonymize successfully, and at least the computer-science research to date seems to support this conclusion.[410] If every person's gait can be uniquely identified by their Fitbit data, then Fitbit data are essentially impossible to de-identify.[411] If every road is unique and therefore a smartphone traveling in a vehicle over any given road emits a unique accelerometer data stream, then accelerometer data are essentially impossible to de-identify.[412] If one can be picked out from 1.5 million anonymized cell-phone location streams based on just a very small number of known locations over a year-long period, then cell-phone location data are essentially impossible to de-identify.[413] If electricity usage can reveal not only that you are watching television but what movie you are viewing, then electricity data are essentially impossible to de-identify.[414]

Internet of Things firms currently act—particularly in their privacy policies—as if "personal information" includes only fields such as name, address, and telephone number.[415] This allows them to use less stringent security to protect sensor data from attack, as well as to release aggregated de-identified sensor data streams to partners or other third parties under the assumption that such information cannot be easily re-identified.[416] But if Internet of Things sensor data are so sparse as to make re-identification fairly simple, such practices are exposing very sensitive consumer information.

At the very least, corporate and privacy counsel for Internet of Things firms should focus on these definitions of PII and consider seriously the possibility that they are currently misleading the public. Several of the privacy policies surveyed, for example, make statements that the firm takes

---

407. *See supra* section II(B)(2).
408. *See supra* section II(B)(2).
409. *See supra* section II(D)(1) and *infra* Appendix.
410. *E.g.*, Lane et al., *supra* note 266; Hardesty, *supra* note 274.
411. *See supra* section II(B)(1).
412. *See supra* notes 275–77 and accompanying text.
413. *See supra* notes 271–74 and accompanying text.
414. *See supra* note 154 and accompanying text.
415. *See supra* subsection II(D)(1)(b) and *infra* Appendix.
416. *See supra* section II(B)(1).

steps to make re-identification of aggregated consumer data impossible.[417] Counsel should investigate whether such promises can actually be upheld, given the ways in which computer-science research has shown sensor data are vulnerable to re-identification.[418]

In addition, regulators—particularly the FTC and California's Office of Privacy Protection—should convene discussions with corporate counsel, computer scientists, academics, and privacy advocates to come up with guidance for the definition of PII in the Internet of Things context. For some types of Internet of Things devices, it may remain plausible to distinguish "personal information" from sensor information. Whether an Internet-connected lightbulb is on or off may not reveal much about a user's identity. But for many—perhaps most—Internet of Things firms, the current approach to defining the concept of PII seems ill-conceived.

3. Protecting Security by Expanding Data-Breach Notification Laws.—Third, regulators, corporate counsel, privacy advocates, and others should focus on data security for the Internet of Things. At the very least, regulators can promulgate soft guidelines on best practices for securing these devices. California already issues such nonbinding guidelines for Internet data generally;[419] it and other states should extend such guidance to the Internet of Things context. Data should be encrypted whenever possible; firmware should be updatable to allow for future measures to address security flaws; and data should be collected, transmitted, and stored only as necessary to make the device function.[420] By giving guidance to Internet of Things firms, regulators can generate interest in and discussion of what constitutes industry standard in this new area.

Beyond that, however, states should extend their data-breach notification laws to reach Internet of Things sensor data. Public disclosure of data breaches serves a reputational sanction function and allows the public to mitigate the harm from data theft.[421] It is essentially a market mechanism to address data security, rather than an administrative one.[422] Coupled with

417. *See supra* section II(D)(1) and *infra* Appendix.

418. *See supra* notes 264–70 and accompanying text.

419. CA. OFFICE OF PRIVACY PROT., RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 8–14 (2012).

420. For example, in response to certain security flaws identified in November 2013, Belkin issued a firmware update for its WeMo home-automation devices. The patch prevented XML injection attacks, added SSL encryption and validation to the WeMo system, and password protected certain port interfaces to prevent malicious firmware attacks. Belkin distributed these updates through its smartphone apps. *See Belkin Fixes WeMo Security Holes, Updates Firmware and App*, NETWORKWORLD (Feb. 19, 2014, 7:16 AM), http://www.networkworld.com/article/2226374/microsoft-subnetelkin-fixes-wemo-security-holes—u/microsoft-subnet/belkin-fixes-wemo-security-holes—updates-firmware-and-app.html, *archived at* http://perma.cc/F4LW-7CSR.

421. Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 917–18 (2007).

422. *Compare* Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 63,

substantive guidance from regulators on data-security best practices for the Internet of Things, data-breach notification can play a powerful role in disciplining device manufacturers.[423] Research has shown that data-breach notification requirements are important to firms and corporate counsel, who take the reputational consequences of such notice seriously.[424]

To extend data-breach notification law to the Internet of Things will require revision of the definitions in existing state statutes. As indicated in Part II, only a few such statutes even arguably apply currently to breach of Internet of Things sensor data.[425] To remedy this, states can take one of two approaches.

First, a state could simply alter the definition of "personal information" in their data-breach statute to include name plus biometric or other sensor-based data such as, but not necessarily limited to, information from fitness and health sensor devices; automobile sensors; home appliance, electricity, and other sensors; and smartphone sensors. This approach would continue the current practice of applying data-breach notification statutes only to *already-identified* datasets—in other words, datasets that include name or other clearly identifying information. As this is the dominant current approach to state data-breach notification laws, it seems likely that were states to consider extending such laws to Internet of Things sensor data, they would continue to require theft of name plus sensitive sensor information.

A second approach would abandon the "name plus" formula, instead triggering data-breach notification if even de-identified datasets were breached. As indicated, most state laws do not currently extend to de-identified datasets.[426] If a state legislature is going to take up revision of their data-breach notification law, however, they might consider the continued wisdom of this limitation. As discussed in the previous section, easy re-identification of Internet of Things data suggests that even de-identified sensor datasets should be protected by data-breach notification statutes. Thus, a state could abandon the name plus approach and trigger notification if de-identified sensor data were stolen.

Either reform would significantly improve on the status quo. Currently, consumers have no way to know whether Internet of Things firms are under attack or if their potentially sensitive information has been stolen. As

66 (2011) (highlighting how data-protection laws help mitigate the market tension between "consumer protection and corporate compliance cost minimization"), *with* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1545 (2013) (describing core aspects of an administrative law approach to cyber security).

423. *See* Burdon, *supra* note 422, at 126–27 (stressing that data-breach notification laws are not ends in themselves, but rather often point to problems and catalyze development of solutions).

424. *See* Bamberger & Mulligan, *supra* note 374, at 275 ("[E]very single respondent mentioned . . . the enactment of state data breach notification statutes[] as an important driver of privacy in corporations." (footnote omitted)).

425. *See supra* notes 323–26 and accompanying text.

426. *See supra* notes 320–29 and accompanying text.

consumers behavior is increasingly measured, quantified, analyzed, and stored by the Internet of Things, it is reasonable that one's weight, heart rate, fertility cycles, driving abilities, and personal habits at home should be protected as much as one's credit card or Social Security number. Such statutory amendment would bring the Internet of Things on par with the way in which we treat other types of sensitive information.

4. Improving Consent by Guiding Internet of Things Consumer Disclosures.—Finally, a fourth initial step would be to provide guidance on how to secure consumer consent to privacy practices on the Internet of Things. Such guidance must come, again, from the FTC, California's Office of Privacy Protection, similar state regulatory bodies, and privacy advocacy groups.

As an initial caveat, I do not want to place too much emphasis on consent as a solution to discrimination, privacy, and security problems. Most regulatory approaches to information privacy suffer from the delusion that consent can sanitize questionable privacy practices. Daniel Solove has called this the "privacy self-management" approach—the belief that providing consumers with sufficient information and control will allow them to "decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information."[427] Unfortunately, privacy self-management fails for a variety of reasons, as Solove and others have shown.[428] Consumers are uninformed, cognitively overwhelmed, and structurally ill-equipped to manage the vast information and myriad decisions that privacy self-management requires.[429]

With that caveat in place, however, focusing on Internet of Things privacy policies is still worthwhile for two reasons. First, consumers and consumer advocates should at least have some *chance* of using privacy policies to assess the implications of product choices. Acknowledging the limitations of consumer use of notice and choice does not justify allowing firms to confuse consumers with poor privacy policies. Second, privacy policies are one of the few regulatory tools currently available.[430] As discussed, the FTC's authority to constrain deceptive practices is a relatively stable ground for regulatory action.[431] Thus, it is worth focusing at least some

427. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

428. *See* Ryan Calo, Essay, *Code, Nudge, or Notice?*, 99 IOWA L. REV. 773, 788–89 (2014) (reviewing the arguments for and against notice requirements).

429. *See id.* at 789 ("Consumers and citizens do not benefit from more information as expected.").

430. *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1028 (2012) ("In the context of digital privacy, notice is among the only affirmative obligations websites face.").

431. *See supra* notes 310–14 and accompanying text.

attention on the ways in which consumer protection law can address Internet of Things privacy policies.

Regulatory guidance must be grounded in protecting consumer expectations in this context. Relatively little empirical research has been done to date exploring those expectations for the Internet of Things.[432] Preliminary research about this new class of devices, however, does reveal certain basic consumer concerns. For example, Pedrag Klasnja and his coauthors studied twenty-eight subjects using fitness trackers over several months.[433] They found that study participants' privacy concerns varied depending on (1) what types of sensors the tracker employed (e.g., accelerometers, GPS, or audio recordings); (2) the length of time data were retained (e.g., kept indefinitely or discarded quickly); (3) the contexts in which the participants used the sensors (e.g., work or home); (4) the perceived value to the participants of the sensor-enabled applications; and (5) whether data were stored on the users' device, on a website, or in the cloud.[434] Similarly, in a recent study of Fitbit, Withings scales, and other health-related sensor devices, Debjanee Barua and her coauthors found that users want to be able to have a copy of the data such devices produce.[435] This is the simplest level of control over one's data—the ability to inspect, manipulate, and store your own information.[436] As the authors note, however, even this basic level of control is not supported by current consumer products: "With the state of present sensors, this is a problem. Typically, each sensor, and its associated data, is under the control of its manufacturer. . . . [T]his does not make it feasible for most people to get a copy of their own data."[437]

Finally, in one of the most interesting studies to date, Heather Patterson and well-known privacy scholar Helen Nissenbaum focused on user expectations of privacy regarding Fitbit and other fitness data.[438] Their study builds on the basic finding that Americans are generally concerned about health-related data being used outside of the medical context: 77% are concerned about such information being used for marketing, 56% are

---

432. *See, e.g.*, Debjanee Barua et al., *Viewing and Controlling Personal Sensor Data: What Do Users Want?*, *in* PERSUASIVE 2013: PROCEEDINGS OF THE 8TH INTERNATIONAL CONFERENCE ON PERSUASIVE TECHNOLOGY 15, 15–16 (Shlomo Berkovsky & Jill Freyne eds., 2013) (using self-reported questionnaires to study people's concerns and reactions to data gathered by sensors and applications).

433. Predrag Klasnja et al., *Exploring Privacy Concerns About Personal Sensing*, *in* PERVASIVE 2009: PROCEEDINGS OF THE 7TH INTERNATIONAL CONFERENCE ON PERSUASIVE COMPUTING 176, 177 (Hideyuki Tokuda et al. eds., 2009).

434. *Id.* at 179–81.

435. Barua et al., *supra* note 432, at 22.

436. *See* Tene & Polonetsky, *supra* note 19, ¶ 64 (explaining how sharing data with consumers allows them to study their own data and draw their own conclusions).

437. Barua et al., *supra* note 432, at 24–25.

438. Patterson & Nissenbaum, *supra* note 239, at 3.

concerned about employer access, and 53% worry about insurer access.[439] Patterson and Nissenbaum found that participants were concerned about the potential for discrimination in hiring and insurance,[440] overly personal marketing efforts based on Fitbit data,[441] and data security.[442] Patterson and Nissenbaum conclude that "[s]elf-tracking services should . . . be concrete about information disclosures, explaining to users the conditions under which *particular* third parties, including employers, insurance companies, and commercial researchers, may obtain access to their data, and giving users the explicit right to opt out of these disclosures."[443]

Together, these studies suggest that Internet of Things consumers want answers to such seemingly basic questions as:

- What exact information does the device collect about itself or its user, using what sorts of sensors?
- Is that information stored on the device itself, on the user's smartphone (assuming the device interacts with the user's phone), on the manufacturer's servers in the cloud, or all of the above?
- Is that information encrypted and how?
- If the information is stored in a de-identified form, does the manufacturer maintain the ability to re-identify the information (for example, in response to a subpoena)?
- Can the user gain access to the raw sensor data in order to export it to another service or device?
- Can the user view, edit, or delete sensor data from the manufacturer's servers, if it is kept there?
- According to the device manufacturer, who owns the data in question?
- Who exactly will the manufacturer or service share the data with, and will the user have any right to opt out of such disclosures?

Such information would provide consumers with the information needed to make informed choices about such connected devices. Unfortunately, subpart II(D) showed that current industry practice provides nothing near this level of disclosure.[444] Instead, existing Internet of Things privacy policies tend to leave unanswered most or all of these basic questions.

---

439. *Id.* at 11 & n.91; *see also* MARKLE FOUND., SURVEY FINDS AMERICANS WANT ELECTRONIC PERSONAL HEALTH INFORMATION TO IMPROVE OWN HEALTH CARE 1, 3 (2006), http://www.markle.org/downloadable_assets/research_doc_120706.pdf, *archived at* http://perma.cc/AAW5-BCW4.

440. Patterson & Nissenbaum, *supra* note 239, at 26–27.

441. *Id.* at 28.

442. *Id.*

443. *Id.* at 46.

444. *See supra* subpart II(D) and *infra* Appendix.

I suggest four basic reforms to current practice, beyond the redefinition of "personally identifiable information" already discussed above.[445] First, regulators should seek industry consensus on best practices for *where* and *when* to give consumers notice about privacy and data issues. Firms should either include the relevant product-related privacy policy in the box with a consumer Internet of Things device or should provide clear information with the product about how a user can find that policy. In addition, firms should clarify whether website policies apply only to website use or also to data generated by product use. If the latter, that merged policy should clearly and directly address the sensor data generated by an Internet of Things device and clarify any distinctions in how such data are handled (as compared to data generated by website use).

Second, Internet of Things privacy policies should commit firms to the principle that consumers own the sensor data generated by their bodies, cars, homes, smartphones, and other devices. As a corollary to this commitment, firms should be encouraged to give users clear access, modification, and deletion rights vis-à-vis sensor data. As indicated in Part II, none of the surveyed privacy policies provided for user ownership of sensor data, and only a very few even addressed access rights to sensor data specifically.[446] Although firms currently sometimes give consumers the right to change "personal information," lack of clarity about whether sensor data qualifies as personal information currently makes those rights relatively weak vis-à-vis sensor data.

Third, Internet of Things privacy policies should specify what sensors are used in a device, exactly what data those sensors create, for what purposes those data are used, and how (and for how long) those data are stored. Consumers should be told whether sensor data are kept on the device or in the cloud, and should be given clear notice that cloud storage means that the data is both more vulnerable to security breach and available for subpoena or other discovery. If sensor data are stored in the cloud, firms should disclose whether such data are stored in encrypted or de-identified form.

Finally, Internet of Things firms should commit not to share even aggregated, de-identified sensor data that poses reasonable risk of re-identification. This is a corollary of my argument in section III(A)(2) for re-defining personally identifiable information in this context, but deserves separate mention. Sensor data are so sensitive and revealing that consumers should be reassured that they will not leak into the public sphere. I would urge regulators and privacy advocates to encourage Internet of Things firms to adopt a simple principle: when in doubt, assume that sensor data can be re-identified. Such firms would do well to build their business models around the assumption that they cannot share even aggregated, de-identified sensor data without significant reputational, market, and regulatory risk.

---

445. *See supra* section III(A)(2).

446. *See supra* section II(D)(1).

These basic reforms to Internet of Things privacy policies are meant to begin a conversation between regulators, consumer advocates, privacy scholars, and corporate counsel. This is a new and evolving field full of new and evolving products. My review of the status quo reveals that reform is necessary to minimize consumer confusion and make Internet of Things privacy policies at least plausibly useful. But this conversation will take time and consensus building between regulators and market players. As the next and final subpart shows, however, the conversation must begin with some urgency.

B. Seize the Moment: Why Public Choice Problems Demand Urgency

This brings us to our final topic: the public choice problems inherent in addressing the Internet of Things and the resulting need for urgency. The informational privacy field has long lamented the difficulties of enacting legislative privacy reforms.[447] Congress has largely ignored academic and even regulatory proposals over the last decade. What chance, then, is there for managing these problems of discrimination, privacy, security, and consent in the Internet of Things context?

There are two reasons for hope. First, sensor-based tracking tends to garner strong responses from the public and its representatives. Various states raced to forbid employers from requiring employees to implant subcutaneous RFID tags even before employers tried.[448] Several states have addressed GPS locational tracking, which galvanizes public reaction.[449] And, as indicated, some states have focused on automobile EDR data and various cross-context use constraints to control sensor data use.[450] In short, sensors tend to scare people—the potential harms they present are perhaps more salient than the more vague or generalized harms of Internet tracking. As a result, reformers may find it easier to mobilize support for shaping the Internet of Things than for cabining Internet or web data generally.

Second, the Internet of Things is relatively new, and therefore industry has perhaps not yet hardened its views on how these data streams should be managed. Lior Strahilevitz has recently noted the importance of identifying winners and losers in privacy contests and of analyzing the public choice issues that thus arise.[451] I have likewise tried to focus informational privacy scholars on these issues.[452] As firms find ways to profit from Internet of Things information, those firms will increasingly push for sparse regulation

---

447. *See, e.g.*, Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 917 (2009) ("Congress remains unable to agree on a data breach notification bill – a perfect illustration, . . . of the slow trajectory of federal privacy legislation.").

448. Peppet, *supra* note 48, at 1202.

449. *Id.* at 1169–70.

450. *See supra* section III(A)(1).

451. Strahilevitz, *supra* note 241, at 2010.

452. *See* Peppet, *supra* note 48, at 1201–03 (discussing public choice problems inherent in regulating privacy).

of such data uses. As the Internet of Things moves from start-ups to large, established Internet players—witness Google's recent acquisition of the Nest Thermostat[453]—those players will have more power to resist shaping of the industry. For now, however, most of the consumer products reviewed in this Article are the work of small, relatively new entrants to this emerging market. Advocates, regulators, and corporate counsel have an opportunity to guide such firms towards best practices. And even as larger firms create Internet of Things products or acquire such devices from start-ups, the newness of this field is likely to temporarily permit some collaboration between those seeking increased regulation and those building the Internet of Things.

This suggests a need for urgency. Not only are consumers currently vulnerable to the discrimination, privacy, security, and consent problems outlined here, but it may become harder over time to address such issues. In technological and political circles it may be convenient to prescribe a "wait and see—let the market evolve" stance, but the reality is that as time passes it will likely become more difficult, not easier, for consumer advocates, regulators, and legislators to act. The Internet of Things is here. It would be wise to respond as quickly as possible to its inherent challenges.

Conclusion

This Article has mapped the sensor devices at the heart of the consumer Internet of Things, explored the four main problems such devices create, and put forth plausible first steps towards constraining those problems. Although my argument's scope is broad, I have tried to show detailed examples of regulatory solutions that have a chance of succeeding in this new arena. As with many such efforts, I am humble in my expectations, hoping mostly to provoke debate and serious consideration of how best to regulate the emerging Internet of Things.

453. *See supra* note 137 and accompanying text.

Appendix
Internet of Things Privacy Policies

Product	Does Product Manual or Quick Start Guide in Packaging Discuss Data, Privacy, or Security?	Privacy Policy: Does Policy . . .							
		Apply to Website Use, Sensor Product Use and Data, or Both?	Discuss Sensor-Data Ownership?	Disclose Sensor Types or Exactly What Sensor Data Are Collected?	Explain Whether Data Are Stored on Device, Smartphone, or Cloud?	Explain Whether Sensor Data Are Encrypted?	Explain Whether Sensor Data Are Stored in De-Identified State, and Whether Firm Has Ability to Re-Identify?	Limit Sensor-Data Use or Resale?	Provide for User to Change or Delete Sensor Data?
Health & Fitness									
Fitbit fitness monitors and Aria Wi-Fi Smart Scale[454]	No	Both	No	No: Sensor information is available on various different pages of website, including on specifications page.[455]	No: One can infer cloud storage but it is not described.	No: Policy mentions "technical and administrative security controls" are used, but does not describe in detail.	No: Policy explains that only aggregated data can be shared with third parties, but does not discuss whether data are stored anonymized.	Unclear whether sensor data are "personal information" under the policy. Personal information can be shared for only limited reasons; Other information can be shared if aggregated and de-identified.	Unclear: User can delete data; however, "Fitbit may continue to use your de-identified data."

454. *Fitbit Privacy Policy*, FITBIT, http://www.fitbit.com/privacy, *archived at* http://perma.cc/ZQ3Q-VNPK.
455. *E.g.*, *Aria Specs*, FITBIT, http://www.fitbit.com/aria/specs, *archived at* http://perma.cc/VCG3-MP2K.

Product	Does Product Manual or Quick Start Guide in Packaging Discuss Data, Privacy, or Security?	Privacy Policy: Does Policy . . .							
		Apply to Website Use, Sensor Product Use and Data, or Both?	Discuss Sensor-Data Ownership?	Disclose Sensor Types or Exactly What Sensor Data Are Collected?	Explain Whether Data Are Stored on Device, Smartphone, or Cloud?	Explain Whether Sensor Data Are Encrypted?	Explain Whether Sensor Data Are Stored in De-Identified State, and Whether Firm Has Ability to Re-Identify?	Limit Sensor-Data Use or Resale?	Provide for User to Change or Delete Sensor Data?
Nike+ FuelBand[456]	No	Both	No	No. Sensor information is available on various different pages of website, including on the specifications page.[457]	No	Somewhat: Policy states that encryption is used for security purposes but implies only credit card information is encrypted.	No	No	Yes, but Nike has the right to keep a copy.

456. *Nike Privacy Policy*, NIKE, http://help-en-us.nike.com/app/answers/detail/article/privacy-policy/a_id/16378/p/3897, *archived at* http://perma.cc/9XZF-VV2T.
457. *E.g.*, *Nike+ Fuelband SE*, NIKE, http://store.nike.com/us/en_us/pd/fuelband-se/pid-924485/pgid-924484, *archived at* http://perma.cc/5JUS-9STF.

Body Media Armband[458]	No	Confusing: Policy states that it applies to website use, but also includes provisions related to sensor data.	Yes: Body Media owns all sensor data.	Somewhat: privacy policy explains that armband data does *not* include location, medical vital signs, or voice data. Does not explain what data are collected. Website includes a page detailing four types of sensor measurements.[459]	No: One can infer cloud storage but it is not described.	Credit card information is encrypted.	Yes: Policy states that armband data is anonymized.	Yes: Limits sale or sharing of personal information, but may sell "non-personally identifiable" information.	No
Withings Blood Pressure Cuff & Weight Scale[460]	No	Both	No	Somewhat: privacy policy explains that arterial pressure or weight data are collected; does not detail sensor types.	No	No	No	Yes: User must consent to sharing of "personal data," which is defined to include sensor data.	Yes

458. *Privacy Policy*, BODYMEDIA, http://www.bodymedia.com/Support-Help/Policies/Privacy-Policy, *archived at* http://perma.cc/9NMT-7EJC.
459. *The Science*, BODYMEDIA, http://www.bodymedia.com/the_science.html, *archived at* http://perma.cc/F99L-YCC2.
460. *Privacy Rules*, WITHINGS, http://www.withings.com/us/privacy-terms, *archived at* http://perma.cc/RBJ4-UN3U.

Product	Does Product Manual or Quick Start Guide in Packaging Discuss Data, Privacy, or Security?	Privacy Policy: Does Policy . . .							
		Apply to Website Use, Sensor Product Use and Data, or Both?	Discuss Sensor-Data Ownership?	Disclose Sensor Types or Exactly What Sensor Data Are Collected?	Explain Whether Data Are Stored on Device, Smartphone, or Cloud?	Explain Whether Sensor Data Are Encrypted?	Explain Whether Sensor Data Are Stored in De-Identified State, and Whether Firm Has Ability to Re-Identify?	Limit Sensor-Data Use or Resale?	Provide for User to Change or Delete Sensor Data?
iHealth Blood Pressure Monitor[461]	No[462]	Two separate policies: one for website and one for products. The latter is referenced in the mobile app Terms of Use, but currently unavailable.	Yes: iHealth owns all sensor data (according to mobile app Terms of Use).	N/A	No, but website indicates data is stored in the cloud.	N/A	N/A	N/A	N/A

461. *Privacy Policy*, iHEALTH®, *supra* note 336; iHEALTH, TERMS AND CONDITIONS, supra note 337.

462. iHEALTH™, WIRELESS BLOOD PRESSURE MONITOR (BP5): OWNER'S MANUAL, *available at* http://www.ihealthlabs.com/files/8514/0192/1706/wireless_bloodpressure_UserManual.pdf, *archived at* http://perma.cc/S268-3FDN; iHEALTH™, WIRELESS BLOOD PRESSURE MONITOR (BP5): QUICK START GUIDE, *available at* http://www.ihealthlabs.com/files/1414/0192/1699/wireless_bloodpressure_QSG.pdf, *archived at* http://perma.cc/ZF2N-MWEH.

Wahoo TICKR Heart Rate Monitor[463]	N/A	Privacy policy only seems to apply to data collected through website.							
BasisPeak Sports Watch[464]	N/A	Both	Somewhat: The policy only mentions that person will be notified if there is a "change in ownership or control" of the data because of a business transition by Basis.	Yes	Yes: Data is initially stored on the device, and stored in the cloud once the device is synched.	No	No	Yes: Basis does not sell or share "personal information to third parties for promotional purposes," but may sell or share "aggregated, de-identified data . . . for marketing purposes or with research organizations."	Yes: Users may contact Basis to request to delete data.

463. *Privacy Policy*, WAHOO FITNESS, http://www.wahoofitness.com/privacy-policy-cookie-restriction-mode, *archived at* http://perma.cc/S5QT-N2QL.
464. *Basis Privacy Policy*, *supra* note 350.

Product	Does Product Manual or Quick Start Guide in Packaging Discuss Data, Privacy, or Security?	Privacy Policy: Does Policy . . .							
		Apply to Website Use, Sensor Product Use and Data, or Both?	Discuss Sensor-Data Ownership?	Disclose Sensor Types or Exactly What Sensor Data Are Collected?	Explain Whether Data Are Stored on Device, Smartphone, or Cloud?	Explain Whether Sensor Data Are Encrypted?	Explain Whether Sensor Data Are Stored in De-Identified State, and Whether Firm Has Ability to Re-Identify?	Limit Sensor-Data Use or Resale?	Provide for User to Change or Delete Sensor Data?
Breathometer[465]	No	Both	No	Yes: Privacy Policy states that BAC tests and location data are collected.	No: One can infer cloud storage but it is not described.	No	No	Yes: Will not sell personal information, but may share non-personally identifiable information.	Yes: Can review but not correct or delete.
JUNE UV Monitor bracelet[466]	N/A	Both	No	No: Sensor information is available on various different pages of website, including on the specifications page.[467]	No: One can infer cloud storage but it is not described.	No	No	Limits sharing somewhat; permits marketing and broadly permits sharing of de-identified data.	Yes: User has access, correction and deletion rights under French law.

465. *Privacy Policy*, BREATHOMETER™, *supra* note 17.

466. *Privacy Policy*, NETATMO, https://www.netatmo.com/en-US/site/terms#div_privacy1, *archived at* http://perma.cc/TB3X-RPFU.

467. *June Specifications*, NETATMO, https://www.netatmo.com/en-US/product/specifications/june, *archived at* http://perma.cc/4468-YWLW.

LifeBEAM Helmet [468]	No	Both	No	No: Sensor information is available on various different pages of website, including on the product page.[469]	No	No	No	Yes: May broadly share non-personal information, but may not sell "potentially personally-identifying and personally-identifying information."	No
Mimo Baby Monitor [470]	N/A	Website and smartphone app. Unclear whether it applies to product data.	No	Policy states that sensors collect biometric information, including skin temperature, body position, and breathing rate; audio; and ambient temperature.	Terms of service explains data are transferred to firm's servers.	Policy states explicitly that sensor data are not encrypted.	No	Limits sharing to aggregate information.	Unclear: User has access, correction and deletion rights for "personal information."
Phyode W/Me bracelet [471]	No [472]	No privacy policy available (although website indicates that one exists).							

468. *LifeBEAM Privacy Policy*, LIFEBEAM, *supra* note 347.
469. *LifeBEAM Helmet*, LIFEBEAM, http://www.life-beam.com/product/helmet/, *archived at* http://perma.cc/6N5U-XV69.
470. *Privacy Policy*, MIMO, *supra* note 349; *Terms of Service*, MIMO, http://mimobaby.com/legal/#TermsOfService, *archived at* http://perma.cc/782Q-GVF4.
471. *Terms of Service*, PHYODE, http://www.phyode.com/terms.html, *archived at* http://perma.cc/G2WS-DMA7.
472. PHYODE, W/ME USER'S MANUAL, *available at* http://www.phyode.com/images/WMe%20Wristband%20User%20Guide.pdf, *archived at* http://perma.cc/EL7Y-5AC8.

Product	Does Product Manual or Quick Start Guide in Packaging Discuss Data, Privacy, or Security?	Privacy Policy: Does Policy . . .							
		Apply to Website Use, Sensor Product Use and Data, or Both?	Discuss Sensor-Data Ownership?	Disclose Sensor Types or Exactly What Sensor Data Are Collected?	Explain Whether Data Are Stored on Device, Smartphone, or Cloud?	Explain Whether Sensor Data Are Encrypted?	Explain Whether Sensor Data Are Stored in De-Identified State, and Whether Firm Has Ability to Re-Identify?	Limit Sensor-Data Use or Resale?	Provide for User to Change or Delete Sensor Data?
Muse headband[473]	No	Both	Yes: User owns biometric or sensor data.	No: Policy mentions some specific examples but otherwise only refers to "[d]ata collected by sensors."	Yes: Policy explains that some data are stored on the local device and in the cloud.	No	Yes: Policy explains that sensor data are stored in an anonymized form.	Unclear: Policy states that sensor data are highly sensitive and implies it will not be shared.	Yes: User can remove or delete biometric or sensor data.

473. *Legal: Privacy Policy*, MUSE™, http://www.choosemuse.com/pages/privacy, *archived at* http://perma.cc/JFR8-UX94.

Propeller Asthma Inhaler Sensor[474]	N/A	Both	Yes: User owns, or has necessary permission to use, "User Content," including data.	Yes: Sensor collects "data regarding inhaler usage."	Yes: Data are collected by app and then stored in the cloud.	No	No	Yes: Propeller Health is a "business associate" under HIPAA and "may not use or disclose your protected health information" without user consent.	No
Automobile									
CarChip[475]	No	Both	No	No	User manual explains that data are stored on user's computer.	No	No	Unclear whether sensor data are personal information; limits sharing of personal information; allows broad sharing of non-personal information.	No: Users can access and correct personal information but no mention of sensor data.

474. *Propeller User Agreement*, *supra* note 339.

475. *Davis Instruments Corp. Privacy Policy*, DAVIS, http://www.davisnet.com/about/policies/privacy/, *archived at* http://perma.cc/7PRD-E868.

Product	Does Product Manual or Quick Start Guide in Packaging Discuss Data, Privacy, or Security?	Privacy Policy: Does Policy . . .							
		Apply to Website Use, Sensor Product Use and Data, or Both?	Discuss Sensor-Data Ownership?	Disclose Sensor Types or Exactly What Sensor Data Are Collected?	Explain Whether Data Are Stored on Device, Smartphone, or Cloud?	Explain Whether Sensor Data Are Encrypted?	Explain Whether Sensor Data Are Stored in De-Identified State, and Whether Firm Has Ability to Re-Identify?	Limit Sensor-Data Use or Resale?	Provide for User to Change or Delete Sensor Data?
Automatic Link driving monitor[476]	N/A	Both	No	Somewhat: It explains types of data collected, including from both the car and device's sensors, but does not specify which exact sensors.	Yes: Policy states that data is stored in the device, in the app, and in its "cloud servers."	No	No	Limits sharing of personal information but not of sensor data.	Yes: User has deletion rights for all data, including sensor data.
BMW iPhone Power Meter App[477]	No policy readily available on iTunes app store or BMW website.								

476. *Legal Information: Privacy Policy*, AUTOMATIC™, *supra* note 354.

477. *BMW M Power Meter*, BMW, http://www.bmw.com/com/en/newvehicles/mseries/x5m/2009/g_meter.html, *archived at* http://perma.cc/8GLD-FZAF (describing the app).

Home & Electric Grid									
Nest Thermostat or Protect[478]		Two separate policies: one for website, one for products.	No	Yes: Policy explains types of information and provides examples.	Yes: Policy states that data are both stored on device and regularly uploaded to Nest "cloud servers."	Yes: Policy states that all data are encrypted.	No	Yes: Limits sharing of personally identifiable information; allows sharing of aggregated and anonymous information.	Somewhat: Allows deletion of personally identifiable information but unclear as to sensor data.
SmartThings home automation sensor system[479]	No: Although available at time of signup for account on mobile app.	Both	No: However, the separate Terms of Service document clarifies that users own sensor data.	Somewhat: Policy provides an example that a home temperature unit would automatically report temperature and location.	Yes: Policy explains that data are automatically stored on servers.	No	No	Only allows sharing of sensor data in de-identified, or de-identified and aggregated form.	Somewhat: User can delete only certain types of information provided by the user.

478. *Privacy Statement*, NEST, *supra* note 344.

479. *Privacy*, SMARTTHINGS, http://www.smartthings.com/privacy/, *archived at* http://perma.cc/FPK9-TBHQ; *Terms of Use*, SMARTTHINGS, http://www.smartthings.com/terms/, archived at http://perma.cc/7BHM-NMFL.

Product	Does Product Manual or Quick Start Guide in Packaging Discuss Data, Privacy, or Security?	Privacy Policy: Does Policy . . .							
		Apply to Website Use, Sensor Product Use and Data, or Both?	Discuss Sensor-Data Ownership?	Disclose Sensor Types or Exactly What Sensor Data Are Collected?	Explain Whether Data Are Stored on Device, Smartphone, or Cloud?	Explain Whether Sensor Data Are Encrypted?	Explain Whether Sensor Data Are Stored in De-Identified State, and Whether Firm Has Ability to Re-Identify?	Limit Sensor-Data Use or Resale?	Provide for User to Change or Delete Sensor Data?
Belkin Wemo Home Automation system[480]	No	Both	No	Somewhat: Policy does not describe sensor types but indicates types of information collected, including usage data, technical information, and environmental data.	Policy indicates that data may be stored in the cloud.	No.	Somewhat: Policy states that usage data are generally anonymized, although it does not indicate whether Belkin stores usage data in an identified form as well.	Limits sale or sharing of Personal Information but defines usage/ sensor data as non-personal information. Permits sharing of aggregated, anonymized non-personal information. Forbids downstream partners from re-identifying data.	Somewhat: Allows access to and deletion of personal information but silent as to sensor data (which it defines as non-personal).

480. *Belkin Privacy Policy*, *supra* note 345.

Connectivity that will shape the future of mission critical IoT applications

06 July, 2015 at 12:00 PM

Posted by: Milan Goldas

There is a lot of discussion around the Internet of Things relating to the lack of standards and managing Big Data, but very little about what is actually at the heart of the IoT: connectivity.

A recent report by Machina Research highlights the challenges the explosion of IoT devices will cause Mobile Network Operators (MNOs). The conclusion is clear; networks are not currently structured to deal with the demands of the IoT, particularly mission critical applications that require maximum reliability. In reality, even if networks were able to quickly scale to meet these demands, relying on one network for global connectivity of mission critical devices is an increasingly risky proposition.

Network pressures
IoT applications for emergency services or healthcare rely on real-time data being sent consistently back to a server, wherever they are located. They behave differently to consumer devices, since they send regular traffic at all times of the day and night. Whilst networks are designed to cope with occasional data peaks, these are usually based on traffic generated by consumer devices. As IoT applications increase, so will the pressure on networks, making them more susceptible to congestion and downtime which is unacceptable for mission critical applications.

Unfortunately, no network is 100% reliable. Technical issues can cause outages which are disastrous for any application. Global connectivity is often provided by a core network with local network agreements in each country. Pricing is therefore dependent on these agreements which are subject to constant fluctuation. These issues could ultimately result in loss of connectivity or the need to swap out the SIMs, a costly exercise especially if devices are located in inaccessible areas. Moreover, many device manufacturers are now using embedded SIMs which require direct control over the profile of the SIM card. The ability to update the connectivity options as market conditions change is essential.

As more devices connect to mobile networks this situation will be exacerbated, so what can developers of IoT applications do to ensure that their connectivity is not compromised by the growth of the IoT itself?

Achieving no single point of failure
The most important requirement for any mission critical application is redundancy. The ability to remotely re-route the data via alternative independent networks is essential to avoid potential problems. The “holy grail” is a no single point of failure solution, whereby the SIM is not only able to connect to multiple networks in each country, it can also swap between different “core” networks on completely separate infrastructures.

Multi-IMSI SIMs go some way to achieving this, however many of these depend on a core IMSI on the SIM, to which relevant IMSIs are sent from the network Home Location Register (HLR) when the device enters a country. This creates additional points of failure, e.g. the HLR or the USSD message used to send the IMSI to the SIM.

The only way to ensure full redundancy is by storing the IMSIs on the SIM card itself. If this solution is combined with an application enabling the SIM to automatically swap between IMSIs when signal is lost, and an Over-The-Air (OTA) platform to remotely swap or add IMSIs to the SIM profile, the solution will not only be redundant, it will also be future proof. As pricing and coverage change, new IMSIs are added to the SIM OTA, and the SIM can remain in the device without the need for expensive SIM swaps or device rebuilds.

This built-in redundancy will allow mission critical applications to grow with the IoT, instead of being hindered by it.

By Charles Towers-Clark, Managing Director of Podsystem Group

As well as strategic planning and corporate governance Charles has direct responsibility

The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

A Notice by the National Telecommunications and Information Administration on 04/06/2016

Action

Notice, Request For Public Comment.

Summary

Recognizing the vital importance of the Internet to U.S. innovation, prosperity, education, and civic and cultural life, the Department of Commerce has made it a top priority to encourage growth of the digital economy and ensure that the Internet remains an open platform for innovation. Thus, as part of the Department's Digital Economy Agenda, the National Telecommunications and Information Administration (NTIA) is initiating an inquiry regarding the Internet of Things (IoT) to review the current technological and policy landscape. Through this Notice, NTIA seeks broad input from all interested stakeholders—including the private industry, researchers, academia, and civil society—on the potential benefits and challenges of these technologies and what role, if any, the U.S. Government should play in this area. After analyzing the comments, the Department intends to issue a "green paper" that identifies key issues impacting deployment of these technologies, highlights potential benefits and challenges, and identifies possible roles for the federal government in fostering the advancement of IoT technologies in partnership with the private sector.

Table of Contents

- DATES:
- ADDRESSES:
- FOR FURTHER INFORMATION CONTACT:
- SUPPLEMENTARY INFORMATION:
- Footnotes

DATES:

Comments are due on or before 5 p.m. Eastern Time on May 23, 2016.

ADDRESSES:

Written comments may be submitted by email to *iotrfc2016@ntia.doc.gov*. Comments submitted by email should be machine-readable and should not be copy-protected. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW., Room 4725, Attn: IOT RFC 2016, Washington, DC 20230. Responders should include the name of the person or organization filing the comment, as well as a page number on each page of their submissions. All comments received are a part of the public record and will generally be posted to *http://www.ntia.doc.gov/category/internet-policy-task-force* without change. All personal identifying information (for example, name, address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information. NTIA will accept anonymous comments.

FOR FURTHER INFORMATION CONTACT:

Travis Hall, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW., Room 4725, Washington, DC 20230; telephone (202) 482-3522; email *thall@ntia.doc.gov*. Please direct media inquiries to NTIA's Office of Public Affairs, (202) 482-7002.

SUPPLEMENTARY INFORMATION:

Background: As part of the Department of Commerce's Digital Economy Agenda, the National Telecommunications and Information Administration (NTIA) is requesting comment on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things (IoT).

Description of IoT and its Impact on the Economy: IoT is the broad umbrella term that seeks to describe the connection of physical objects, infrastructure, and environments to various identifiers, sensors, networks, and/or computing capability.[1] In practice, it also encompasses the applications and analytic capabilities driven by getting data from, and sending instructions to, newly-digitized devices and components.

Although a number of architectures describing different aspects or various applications of the IoT are being developed, there is no broad consensus on exactly how the concept should be defined or scoped. Consensus has emerged, however, that the number of connected devices is expected to grow exponentially, and the economic impact of those devices will increase dramatically.[2] While some types of devices will fall into readily identifiable commercial or public sectors in their own right—for example, implantable health devices—most will serve the function of enabling existing industries to better track, manage, and automate their core functions. The potential health, safety, environmental, commercial, and other benefits of IoT are enormous, from reducing the risk of automobile-related injuries and fatalities to enabling micro-cell weather forecasting. IoT has the potential to catalyze new user applications and give rise to new industries. For example, IoT is the foundation for “Smart Cities” efforts, which use

pervasive connectivity and data-driven technologies to better manage resources, meet local challenges, and improve quality of life.

However, the IoT also presents challenges,[3] which in turn have begun to generate initial thinking and policy responses both inside and outside of government. A number of Federal agencies—for example, the National Highway Traffic Safety Administration (NHTSA) and the Food and Drug Administration (FDA)—have already begun grappling with potential health, safety, and security issues arising from the connection of cars and medical devices to the Internet.[4] The Federal Trade Commission (FTC) has identified privacy and cybersecurity aspects of IoT, and proposed some possible best practices.[5] Pursuant to the White House Smart Cities Initiative, the U.S. Government is providing $35 million in new grants and nearly $70 million in new spending on Smart Cities across several departments.[6] Additional activities at the federal level seek to take advantage of the potential opportunities as well as address any possible issues raised by the deployment of IoT in relation to agency missions. IoT has also garnered interest by other national governments, standards organizations, and intergovernmental organizations that are interested in understanding how to engage in the IoT ecosystem to encourage economic growth and innovation.[7] Unfortunately, country specific strategies threaten the possibility of a global patchwork of approaches to IoT, which would increase costs and delay the launch of new products and services, dampening investment. The U.S. government will need to work with stakeholders to develop industry-driven solutions; however, thus far no U.S. government agency is taking a holistic, ecosystem-wide view that identifies opportunities and assesses risks across the digital economy.

The Department's Digital Economy Initiatives: More than six years ago, the Department created the Internet Policy Task Force (IPTF) to identify and address leading public policy and operational challenges in the Internet ecosystem. The IPTF collaborates across bureaus at the Department, seeks public comment, and has produced policy papers on a variety of important topics.

In recognition of the broad impact that the Internet and digitization are having across the economy, in 2015 the Department created the Digital Economy Leadership Team (DELT). Comprised of senior officials from across the Department, the DELT provides high-level guidance and coordination, leveraging the substantial expertise within the agency to promote initiatives that have a positive impact on the digital economy and society. The DELT currently focuses on the four pillars of the Department's 2015-16 Digital Economy Agenda: promoting a free and open Internet worldwide; promoting trust and confidence online; ensuring Internet access for workers, families, and companies; and promoting innovation in the digital economy. Working closely together, the DELT and IPTF ensure that the Department is helping businesses and consumers realize the potential of the digital economy to advance growth and opportunity.

Given the cross-cutting nature of the IoT landscape, the Department of Commerce—through the DELT and IPTF—is able to provide important perspective and expertise on IoT. The mission of the Department is to help establish conditions that will enable the private sector to grow the economy, innovate, and create jobs. The Department also has statutory authority, expertise, and ongoing work streams in numerous areas that are critical to the development of IoT, including: cybersecurity, privacy, cross-border data flows, spectrum, international trade, advanced

manufacturing, protection of intellectual property, standards policy, Internet governance, big data, entrepreneurship, and worker skills. For example:

- The Department has long standing technological and policy expertise and experience that it is applying to IoT. The Department's National Institute of Standards and Technology (NIST) has coordinated the development of a draft reference architecture for Cyber-Physical Systems and is conducting a Global City Teams Challenge to foster the development of Smart Cities and promote interoperability. NTIA's spectrum planning and management activities contemplate the growth of IoT and its Institute for Telecommunications Sciences (ITS) has begun testing the possible effects of IoT on spectrum usage. Both NIST and NTIA have been actively engaged with international standards bodies and international organizations on aspects of IoT and other related areas (*e.g.,* cybersecurity), and have been further engaged with other Federal agencies.
- The Economic Development Administration (EDA) provides grants to communities around the country to build up their technology-focused innovation ecosystems in order to grow their local economies and create jobs.
- The U.S. Patent and Trademark Office (USPTO) continues to improve its patent quality, especially in new technological domains, including IoT. USPTO also plays a key role in the alignment of intellectual property policies around the world, so that U.S. inventors of IoT technology can have access to the protections they need to continue innovating and sell their products and services everywhere.
- The International Trade Administration (ITA) is an active promoter of IoT and Smart Cities on the international stage, including participation in the CS Europe Smart Cities Initiative and working with the other Federal agencies to consider innovative financing mechanisms for Smart City projects. ITA hosts roundtables on an ad hoc basis with the private sector and federal partners to discuss Smart Cities and infrastructure financing. In addition, ITA's Office of Textiles and Apparel is holding a Smart Fabrics Summit (*http://smartfabricssummit.com/*) on April 11, 2016.

The Department, through this RFC and subsequent green paper, will capitalize on the Department's experience and holistic economic perspective to craft an approach to IoT and its potential impacts that will best foster IoT innovation and growth. Where relevant, comments received may also inform the work of other federal initiatives, such as the recently created Commission on Enhancing National Cybersecurity.

Request for Comment:

Instructions for Commenters: The Department invites comment on the full range of issues that may be presented by this inquiry, including issues that are not specifically raised in the following questions. Commenters are encouraged to address any or all of the following questions. To the extent commenters choose to respond to the specific questions asked, responses should generally follow the below structure and note the number corresponding to the question. Comments that contain references to studies, research, and other empirical data that are not widely published should include copies of the referenced materials with the submitted comments.

For any response, commenters may wish to consider describing specific goals or actions that the Department of Commerce, or the U.S. Government in general, might take (on its own or in conjunction with the private sector) to achieve those goals; the benefits and costs associated with

the action; whether the proposal is agency-specific or interagency; the rationale and evidence to support it; and the roles of other stakeholders.

General:

1. Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?

a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?

b. What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why?

c. What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?

2. The term "Internet of Things" and related concepts have been defined by multiple organizations, including parts of the U.S. Government such as NIST and the FTC, through policy briefs and reference architectures.[8] What definition(s) should we use in examining the IoT landscape and why? What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?

3. With respect to current or planned laws, regulations, and/or policies that apply to IoT:

a. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?

b. Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?

4. Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: Consumer vs. industrial; public vs. private; device-to-device vs. human interfacing.

5. Please provide information on any current (or concluded) initiatives or research of significance that have examined or made important strides in understanding the IoT policy landscape. Why do you find this work to be significant?

Technology: Technology is at the heart of IoT and its applications. IoT development is being driven by a very diverse set of stakeholders whose expertise in science, research, development, deployment, measurements and standards are enabling rapid advances in technologies for IoT. It

is important to understand what technological hurdles still exist, or may arise, in the development and deployment of IoT, and if the government can play a role in mitigating these hurdles.

6. What technological issues may hinder the development of IoT, if any?

a. Examples of possible technical issues could include:

i. Interoperability

ii. Insufficient/contradictory/proprietary standards/platforms

iii. Spectrum availability and potential congestion/interference

iv. Availability of network infrastructure

v. Other

b. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

7. NIST and NTIA are actively working to develop and understand many of the technical underpinnings for IoT technologies and their applications. What factors should the Department of Commerce and, more generally, the federal government consider when prioritizing their technical activities with regard to IoT and its applications, and why?

Infrastructure: Infrastructure investment, innovation, and resiliency (such as across the information technology, communications, and energy sectors) will provide a foundation for the rapid growth of IoT services.

8. How will IoT place demands on existing infrastructure architectures, business models, or stability?

9. Are there ways to prepare for or minimize IoT disruptions in these infrastructures? How are these infrastructures planning and evolving to meet the demands of IoT?

10. What role might the government play in bolstering and protecting the availability and resiliency of these infrastructures to support IoT?

Economy: IoT has already begun to alter the U.S. economy by enabling the development of innovative consumer products and entirely new economic sectors, enhancing a variety of existing products and services, and facilitating new manufacturing and delivery systems. In light of this, how should we think of and assess IoT and its effects *?* The questions below are an effort to understand both the potential economic implications of IoT for the U.S. economy, as well as how to quantify and analyze the economic impact of IoT in the future. The Department is interested in both the likely implications of IoT on the U.S. economy and society, as well as the tools that could be used to quantify that impact.

11. Should the government quantify and measure the IoT sector? If so, how?

a. As devices manufactured or sold (in value or volume)?

b. As industrial/manufacturing components?

c. As part of the digital economy?

i. In providing services

ii. In the commerce of digital goods

d. In enabling more advanced manufacturing and supply chains?

e. What other metrics would be useful, if any? What new data collection tools might be necessary, if any?

f. How might IoT fit within the existing industry classification systems? What new sector codes are necessary, if any?

12. Should the government measure the economic impact of IoT? If so, how?

a. Are there novel analytical tools that should be applied?

b. Does IoT create unique challenges for impact measurement?

13. What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture?

a. What will be the benefits, if any?

b. What will be the challenges, if any?

c. What role or actions should the Department of Commerce and, more generally, the federal government take in response to these challenges, if any?

14. What impact (positive or negative) might the growth of IoT have on the U.S. workforce? What are the potential benefits of IoT for employees and/or employers? What role or actions should the government take in response to workforce challenges raised by IoT, if any?

Policy Issues: A growing dependence on embedded devices in all aspects of life raises questions about the confidentiality of personal data, the integrity of operations, and the availability and resiliency of critical services.

15. What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?

16. How should the government address or respond to cybersecurity concerns about IoT?

a. What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns?

b. How do these concerns change based on the categorization of IoT applications (*e.g.*, based on categories for Question 4, or consumer vs. industrial)?

c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?

17. How should the government address or respond to privacy concerns about IoT?

a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?

b. Do these concerns change based on the categorization of IoT applications (*e.g.*, based on categories for Question 4, or consumer vs. industrial)?

c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

18. Are there other consumer protection issues that are raised specifically by IoT? If so, what are they and how should the government respond to the concerns?

19. In what ways could IoT affect and be affected by questions of economic equity?

a. In what ways could IoT potentially help disadvantaged communities or groups? Rural communities?

b. In what ways might IoT create obstacles for these communities or groups?

c. What effects, if any, will Internet access have on IoT, and what effects, if any, will IoT have on Internet access?

d. What role, if any, should the government play in ensuring that the positive impacts of IoT reach all Americans and keep the negatives from disproportionately impacting disadvantaged communities or groups?

International Engagement: As mentioned earlier, efforts have begun in foreign jurisdictions, standards organizations, and intergovernmental bodies to explore the potential of, and develop standards, specifications, and best practices for IoT. The Department is seeking input on how to best monitor and/or engage in various international fora as part of the government's ongoing efforts to encourage innovation and growth of the digital economy.

20. What factors should the Department consider in its international engagement in:

a. Standards and specification organizations?

b. Bilateral and multilateral engagement?

c. Industry alliances?

d. Other?

21. What issues, if any, regarding IoT should the Department focus on through international engagement?

22. Are there Internet governance issues now or in the foreseeable future specific to IoT?

23. Are there policies that the government should seek to promote with international partners that would be helpful in the IoT context?

24. What factors can impede the growth of the IoT outside the U. S. (*e.g.,* data or service localization requirements or other barriers to trade), or otherwise constrain the ability of U.S. companies to provide those services on a global basis? How can the government help to alleviate these factors?

Additional Issues:

25. Are there IoT policy areas that could be appropriate for multistakeholder engagement, similar to the NTIA-run processes on privacy and cybersecurity?

26. What role should the Department of Commerce play within the federal government in helping to address the challenges and opportunities of IoT? How can the Department of Commerce best collaborate with stakeholders on IoT matters?

27. How should government and the private sector collaborate to ensure that infrastructure, policy, technology, and investment are working together to best fuel IoT growth and development? Would an overarching strategy, such as those deployed in other countries, be useful in this space? If the answer is yes, what should that strategy entail?

28. What are any additional relevant issues not raised above, and what role, if any, should the Department of Commerce and, more generally, the federal government play in addressing them?

Dated: April 1, 2016.

Lawrence E. Strickling,

Assistant Secretary for Communications and Information.

[FR Doc. 2016-07892 Filed 4-5-16; 8:45 am]

BILLING CODE 3510-60-P

Footnotes

1. The term was initially coined by Kevin Ashton in 1999 in a presentation at Proctor and Gamble in reference to radio-frequency identification tags (RFIDs). *See* Kevin Ashton, *That `Internet of Things' Thing,* RFID Journal (June 22, 2009), *http://www.rfidjournal.com/articles/view?4986*.

2. In 2003, there were only around 500 million connected devices, but by 2015 there were around 25 billion connected devices. Devices now outnumber people by 3.5 to 1. (Intel, *A Guide to the Internet of Things Infographic,* available at *http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html*). It is expected by 2020 that there will be up to 200 billion connected devices and these devices will outnumber people by 26 to 1. The McKinsey Global Institute estimates that the cross-sector impact of IoT technologies will be between $3.9 trillion and $11 trillion by 2025. *See* James Manyika et al, *Unlocking the Potential of the Internet of Things,* McKinsey & Co. (June 2015), *http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world*.

3. See, for example, the concerns laid out by the National Security Telecommunications Advisory Committee (NSTAC) in *NSTAC Report to the President on the Internet of Things* (Nov. 2014), pg. 21-22. *https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf*.

4. *See* U.S. Dept. of Health and Human Services, *Radio Frequency Wireless Technology in Medical Devices: Guidance for Industry and Food and Drug Administration Staff* (Aug. 14, 2013), *http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf;* see also NHTSA, *Vehicle-to-Vehicle Communications* (last accessed March 9, 2016), *http://www.safercar.gov/v2v/index.html*.

5. Federal Trade Comm'n, *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks,* FTC (Jan. 27, 2015), *https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices*.

6. The White House, *FACT SHEET: Administration Announces New "Smart Cities" Initiative to Help communities Tackle Local Challenges and Improve City Services,* The White House Office of the Press Secretary (Sept. 14, 2015), *https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help*.

7. For example, the Internet Engineering Task Force (IETF), International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and ISO and IEC's Joint Technical Committee 1 (ISO/IEC JTC1) and the International Telecommunications Union's Standardization Sector (ITU-T) have initiated discussion and work related to IoT.

8. Federal Trade Comm'n, *Internet of Things: Privacy and Security in a Connected World*, FTC (Jan. 2015), *https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*; Abdella Battou, *CPS PWG: Reference Architecture*, National Institute of Standards and Technology (accessed March 9, 2016), *http://www.nist.gov/cps/cpspwg_refarch.cfm*.

10 Policy Principles for Unlocking the Potential of the Internet of Things

By Daniel Castro & Joshua New | December 4, 2014

Summary: "The Internet of Things" encapsulates the idea that ordinary objects will be embedded with sensors and connected to the Internet. To date, most discussion of the Internet of Things has highlighted the technology; to the extent it has addressed policy, the focus has been largely negative (i.e. how to limit the supposed risks from deployment). In contrast, this report highlights principles that policymakers in all nations need to apply in order to maximize the considerable promise of the Internet of Things for economic growth and social well-being. Of two conflicting approaches to the Internet of Things, neither: the "impose precautionary regulations" nor the counter "leave it completely up to the market" will allow societies to gain the full benefits from the Internet of Things revolution. This report presents ten principles to help policymakers establish policies and programs to support and accelerate the deployment and adoption of the Internet of Things.

The success of the Internet today can be credited in part to policymakers actively taking a role to ensure its growth, and this same approach should to be applied to build the Internet of Things.

The Internet of Things encapsulates the idea that ordinary objects—from thermostats and shoes to cars and lamp posts—will be embedded with sensors and connected wirelessly to the Internet. These devices will then send and receive data which can be analyzed and acted upon. As the technology becomes cheaper and more robust, an increasing number of devices will join the Internet of Things. Though many of the changes to everyday devices may be subtle and go unnoticed by consumers, the long-term effect could ultimately have an enormously positive impact on individuals and society. A connected world is capable of anything from improving personal health to reducing pollution to making industry more

productive. The Internet of Things offers solutions to major social problems, but this vision of a fully connected world will not be achieved without initiative and leadership from policymakers to promote its deployment and avoid pitfalls along the way.

The potential size and scope of the Internet of Things is enormous, with over 16 billion devices estimated to be in use today, and many more to come.[1] By 2020, the total worldwide count is expected to reach over 40 billion.[2] This growth is visible across practically every industry. By 2020, the number of wearable devices will surpass 100 million, the number of Internet-connected cars will exceed 150 million, and the number of connected wireless lights will reach 100 million—to name just a few.[3]

The magnitude of the benefits brought by the Internet of Things is also impressive, and this technology may improve nearly every aspect of life. Consider the benefits of smart homes. Connected devices that automatically regulate electricity usage based on whether anyone is home can cut energy usage and bills.[4] Smart meters can send dynamic price signals to smart appliances to reduce peak energy consumption.[5] Connected sensors can improve home safety by detecting fires and other emergencies more quickly and reliably than traditional methods, alerting authorities sooner.[6] Blinds that automatically detect and filter out sunlight, smart heating and cooling systems that can maintain different rooms at different temperatures, and lighting that automatically adapts to time of day and can be controlled from a smartphone will make home life more comfortable than ever before.[7]

Connected devices can also provide consumers important new insights about their health and fitness. Companies are designing wearables for every stage of life from smart "onesies" with embedded sensors that help parents monitor their infants' health to activity sensors that allow elderly adults to live safely and independently. Wearable biometric monitors can help individuals track their health, monitor chronic medical conditions, and improve health care outcomes.[8] In addition, fitness trackers such as FitBit and Nike FuelBand can help consumers be more active and engage in healthy behaviors.[9]

Local leaders can help build smart cities by integrating the Internet of Things into public buildings and infrastructure, including roadways, transit systems, and utilities. These technologies can help make cities safer, more sustainable, and more resilient while also providing new economic opportunities for their residents. For example, networked sensors can monitor the structural integrity of bridges and highways in real time to prevent catastrophes from happening and encourage cost-savings through timely preventative maintenance.[10] And, intelligent transportation systems

can make roads safer, facilitate traffic flow, and make public transportation more efficient.[11]

Industries that restructure their practices around the Internet of Things can improve productivity and sustainability. With everything from networked assembly lines that track every screw turn to ensure quality control and safety to connected supply chains that reduce downtime and ensure transparency in material sourcing, the Internet of Things will increase industry competitiveness.[12] The increased capacity for data collection from the Internet of Things brings benefits as well. Insurers can use actuarial models that factor in data from connected devices to better understand risk and reduce costs for their customers. Companies can monitor and enhance the safety of their workers in real time and prevent accidents.

Overall, global spending on the Internet of Things is predicted to grow to approximately $3 trillion by 2020.[13] Of course, any capital equipment represents a cost, not a benefit. In that businesses and consumers purchase technology only if benefits exceed costs and because many benefits extend beyond the immediate purchasers to the entire network, the overall economic benefits from the Internet of Things will be even more significant.[14]

As technological barriers decrease and adoption of the Internet of Things takes off, its potential benefits depend in part on how policymakers respond to this technology. There are four main approaches policymakers could employ regarding the Internet of Things:

1. Precautionary regulations: Some policymakers focus on the potential risks associated with the Internet of Things and want to regulate it accordingly. These policymakers believe that preemptive regulations will increase consumer trust and therefore increase adoption, but the reality is that heavy-handed rules would likely imposes costs, limit innovation, and slow adoption.

2. No intervention: Some policymakers resist laws and regulations for the Internet of Things because they believe the free market operating independently of government interventions achieves the maximum possible consumer benefit. However, by avoiding all interventions, policymakers miss the opportunity to proactively support the deployment of the Internet of Things.

3. Indigenous innovation: Some policymakers view the Internet of Things as an opportunity to create export opportunities for domestic firms. These policymakers may endorse policies that hinder foreign companies from competing in the domestic market, such as

adopting national technical standards rather than adopting international ones.[15] Such policies are anti-competitive and create fragmented markets for the Internet of Things.

4. Technology champions: Some policymakers have taken a proactive role in accelerating the development and deployment of the Internet of Things, such as by funding research on sensor networks, creating pilot projects for smart cities, preventing over-regulation of wearable health technologies, and providing incentives for smart grid deployment. These policymakers see government as a critical partner in promoting the benefits that come from using these technologies.

Recognizing the inherent shortcomings and limitations of some of these approaches is crucial to developing sound policy for the Internet of Things. The status of the Internet of Things as an emerging technology necessitates a policy framework that is fully cognizant of its benefits, allows for future innovation, and responsibly protects against misuse without restricting its capacity to deliver social, civic, and economic benefits.

10 POLICY PRINCIPLES FOR THE INTERNET OF THINGS

1. CHART THE COURSE FOR ADOPTION

Every nation should develop a strategic roadmap to guide the deployment and adoption of the Internet of Things. In addition to a comprehensive roadmap, national agencies involved in specific sectors can develop targeted action plans for particular industries. In the United States, for example, the Department of Housing and Urban Development should develop an action plan to promote smart homes, and the Department of Energy should develop a plan to improve energy efficiency with connected devices. The private sector will be more likely to embrace the Internet of Things if government leaders are paving the way for deployment.

Policymakers should actively work to overcome barriers to adoption, such as security risks or a lack of interoperability. For example, electronic health records should be able to integrate data from wearable medical devices and the government can promote industry adoption of voluntary cybersecurity principles to protect consumer data. Since many of the benefits from the Internet of Things will occur with widespread adoption, policymakers should promote efforts to develop global, industry-led standards and oppose efforts to develop nation-specific standards. To maximize the potential benefits of data analytics, developers should also

be able to easily share and integrate data across organizational, political, and geographic boundaries.

2. LEAD BY EXAMPLE

The government should be an early adopter of the Internet of Things to demonstrate the benefits of the technology. From sewers to streetlights, government agencies should make "smart" the default for all new investments and allocate funding for smart city demonstration projects. For example, all government infrastructure projects should incorporate the Internet of Things into their design. Investing in smart technology for public infrastructure projects will increase safety, reduce maintenance costs, and improve operations. In addition, these projects will generate valuable data that should be made available to the public.

To maximize the benefits of the Internet of Things, government agencies should restructure their practices around the new capabilities offered by the technology. Public services that incorporate connected sensors can provide important benefits to the public. For example, the city of Buffalo, New York uses sensor-equipped snow plows to respond to citizens' snow-clearing requests more quickly and to target problem areas more efficiently.[16] And, government agencies that perform inspections of equipment and facilities can use the Internet of Things to perform their duties more quickly and effectively. For example, the U.S. Department of Agriculture (USDA) approved new regulations to allow advanced imaging sensors to evaluate food safety and quality. As a result, a single poultry food safety inspector can now process 175 birds per minute, up from a previous speed of 35 birds per minute, a substantial gain in efficiency.[17]

3. LOOK TO PARTNERSHIPS TO OVERCOME OBSTACLES

Many Internet of Things projects will benefit from government agencies establishing partnerships with both the private sector and others in government. In particular, funding these types of projects can be challenging for cities with limited budgets. For example, a city may not have the budget to install smart streetlamps, even if they would end up paying for themselves in energy savings. Innovative partnerships whereby the private sector pays for, builds, and manages certain technology projects while receiving a portion of the savings can allow local leaders to deliver the Internet of Things and its benefits in situations where budget constraints would have otherwise impeded progress. For example, the city of Mumbai, India partnered with a smart metering company to help with its failing water infrastructure that was leaking 50 percent of its water a day. For the same amount of money the government would have spent patching new leaks without ever improving the overall integrity of the system, the partnership with the metering company cut the water loss in half.[18]

4. REDUCE REGULATORY BARRIERS AND DELAYS FOR GETTING SMART DEVICES TO MARKET

A lengthy and cumbersome regulatory review process that increases the time to market for smart devices can discourage entrepreneurs from developing new and potentially lifesaving products. Wearable technologies can allow individuals to spend less time in the hospital, receive better treatments, and more easily monitor their personal health. Since subjecting these technologies to lengthy regulatory review processes can delay these benefits from reaching consumers, policymakers should work to ensure that these processes are as efficient as possible. Moreover, most of these technologies will undergo continuous innovation and improvement and the regulatory review process should allow for, and encourage, upgrades. In a clear example of a review process with room for improvement, it takes on average over two and a half years for the U.S. Food and Drug Administration to approve a low-risk medical device, compared to an average of seven months in Europe.[19] These delays can cost a company an average of $500,000 per month and discourage entrepreneurs from bringing products to market.[20] While consumer safety should remain a top priority, the human cost of delaying lifesaving technology should not be ignored.

5. MINIMIZE THE REGULATORY COST OF DATA COLLECTION

Policymakers should create laws and regulations that allow businesses and governments to build products and services efficiently, using the highest quality, most complete data possible. For example, obtaining explicit consent for data collection would be an unnecessary cost for the vast majority of applications of the Internet of Things that pose no real threat to consumer welfare. Regulations requiring individuals manually to give consent to data collection would impose costs on companies that ultimately would be passed on to consumers. Instead, the standard method of data collection for the Internet of Things should be “opt out”; this would ensure that the data is accurate, complete, and useful, yet still provide those who wish not to share their data that option.

Similarly, policymakers should recognize that consumers do not benefit from being inundated with notices, especially since most data collection would be routine and insignificant. Rather than require that all devices directly notify consumers of their policies and terms of service, companies should simply make this information available to those who wish to read it. This type of shift is especially important since many devices that will make up the Internet of Things will have only a small display or no display at all.

6. MAKE IT EASY TO SHARE AND REUSE DATA

The Internet of Things will generate an unprecedented quantity of data, and policymakers should be careful not to equate simple data sharing with harmful misuse. Data collected from connected devices offer a myriad of potential benefits to consumers, clinicians, researchers, government agencies, and commercial entities, and if these datasets are shared, these benefits are multiplied. There may be one primary reason to collect data, but one hundred good applications of this data beyond its initial purpose. In order to maximize the social and economic benefits of information, data users of all kinds acting in good faith must be able to share and reuse data with ease.

As governments at the municipal, state, and federal levels integrate connected devices into public infrastructure and government services, the de-identified data they collect should be treated as a public resource and shared with the public accordingly. Making this data easy to access, such as through portals and application programming interfaces (APIs), and free to reuse without restrictions creates tremendous opportunity for private-sector innovation, academic research, and improvements in government transparency.[21] The city of Chicago, which has been integrating the Internet of Things into city infrastructure and services as part of its Array of Things project, has made over 600 machine- and human-readable datasets freely available online.[22] With this new resource, citizens have been able to more easily navigate public transit, the city's pest-control agency has reduced the rat population, and the police have created predictive models to fight crime more effectively.[23]

Since the full potential benefits of the Internet of Things will not be realized until data from interconnected technology are widely used, policymakers should incentivize both individuals and the private sector to share data. For example, governments can support the development of new tools and techniques to properly de-identify different types of data so that they are still useful for analysis.[24] Where possible, companies should be encouraged to provide consumers access to their data to stimulate the development of new applications. For example, the U.S. Department of Energy's green button initiative gives consumers access to their energy usage data and allows them to share their data with third-party developers who provide services such as virtual energy audits.[25] Policymakers should also work to ensure data can flow across borders and eliminate digital barriers to trade, such as data residency requirements and other localization policies.

7. RELENTLESSLY PURSUE BETTER DATA

With ever-higher-quality sensors and an increasing number of them, the Internet of Things allows for the capture of an unprecedented quantity and

quality of data. Policymakers should continue to invest in opportunities to collect more granular, timely, and complete data. Government agencies should use better data to better monitor internal processes and improve productivity and outcomes. For example, police departments can use sensors to better monitor the safety of their officers in real time and to hold officers responsible for their actions. Port authorities can use sensors to better protect the border by tracking containers and shipments coming into the country. Better data enables not only a more effective government, but a more transparent one as well.

8. REDUCE THE "DATA DIVIDE"

Policymakers should encourage widespread adoption of connected devices, from wearable fitness trackers to sensors on street corners, to close the "data divide"—the social and economic inequalities that may result from a lack of collection and use of data about an individual or community.[26] The goal of policymakers should be to ensure that no groups are systematically excluded from data collection activities so that all individuals have the opportunity to obtain the social and economic benefits of data. Policymakers should work to develop programs to ensure that all communities can benefit from the Internet of Things. For example, funding for smart city infrastructure should be made available to a diverse set of neighborhoods, including low-income ones.

9. USE DATA TO TACKLE HARD PROBLEMS

While the Internet of Things offers many economic benefits, policymakers need to ensure that opportunities to use these devices to address important social issues, such as health care and public safety, are also a top priority. For example, aggregate data from personal fitness devices can provide health officials with unprecedented insights into public health. Tracking changes in biometric readings across a city could even help identify the spread of deadly outbreaks, helping public officials better contain diseases and start treating sick individuals earlier. As Google's CEO and co-founder Larry Page has noted, public squeamishness over mining of health data likely costs around 100,000 lives a year.[27] Policymakers should support efforts to collect and aggregate data on a large scale to solve collective problems.

Networked sensors can detect flooding and trigger emergency responses more quickly.[28] Wearable technologies and sensors on street corners can give new insights onto air quality on a block-by block- basis and help develop strategies to curb pollution.[29] The list of ways public welfare could be enhanced by the Internet of Things is long, but if it is to be fully effective in addressing these problems, policymakers should shift their focus to the problem-solving capabilities of smart devices.

10. WHERE RULES ARE NEEDED TO PROTECT CONSUMERS, KEEP THEM NARROW AND TARGETED

Many technologies are often met with fear, uncertainty, and doubt, especially by those who are unfamiliar with them or opposed to change. Policymakers cannot afford to succumb to these forces if they expect to enable society to take full advantage of the Internet of Things. In particular, policymakers should be extremely cautious about regulating on the basis of purely speculative concerns that might not even come to pass, especially when doing so might curtail substantial economic and social benefits, many of which are already being realized today.[30] Most hypothetical concerns are likely to never become realities if factors such as market forces, cultural norms, and new technologies, intervene. In addition, existing laws, such as anti-discrimination statutes, often protect individuals from certain types of abuses and harms.

However, policymakers should intervene promptly if specific problems arise. In doing so, they should be careful to ensure that their rulemaking targets specific, demonstrated harms. Attempting to erect precautionary regulatory barriers for purely speculative concerns is not only unproductive, but it can discourage future beneficial applications of the Internet of Things. For example, privacy activists raised objections when several cities made plans to install gunshot detection equipment in public spaces. However, the effectiveness of these technologies in reducing gun crime has proven to be incredibly valuable to law enforcement.[31]

CONCLUSION

These ten policy principles serve as a blueprint for Internet of Things policies that promote adoption, increase the value of data collected from connected devices, and maximize the benefits of the Internet of Things for consumers, government, and industry. While many of the future challenges of the Internet of Things may still be unknown, a policy framework built around these principles should maximize the benefits from the Internet of Things. The success of the Internet today can be credited in part to policymakers actively taking a role to ensure its growth, and this same approach should to be applied to build the Internet of Things.

REFERENCES

1. "The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020," ABI Research, August 20, 2014, https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect.

2. Ibid.

3. Jolyon Barker, Paul Lee, and Duncan Steward, "Technology, Media & Telecommunications Predictions 2014," Deloitte, 2014, http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-predictions-2014.pdf and Keith Bloomberg, "The Race to Market the Connected Car," Automotive News, January 10, 2014, http://www.autonews.com/article/20140110/OEM06/301109910/the-race-to-market-the-connected-car, "100 Million Internet Connected Wireless Lights by 2020," ON World, November 20, 2013, http://onworld.com/news/100-Million-Internet-Connected-LED-Lights-by-2020.html.

4. Ilana Greene, "Smart Houses Help Reduce Energy Use and Save Money," Huffington Post, December 19, 2013, http://www.huffingtonpost.com/ilana-greene/smart-houses-help-reduce_b_4472919.html.

5. Austin Harney, "Smart Metering Technology Promotes Energy Efficiency for a Greener World" Analog Dialogue, Volume 43-01, January 2009, http://www.analog.com/library/analogdialogue/archives/43-01/smart_metering.pdf.

6. Juhwan Oh, Zhongwei Jiang, and Henry Panganiban, "Development of a Smart Residential Fire Protection System, Advances in Mechanical Engineering, Volume 2013, 2013, http://www.hindawi.com/journals/ame/2013/825872/.

7. Jason Chen, "Home Automation! What You Need to Know to Not Be Dumb," Gizmodo, September 27, 2010, http://gizmodo.com/5647352/home-automation-what-you-need-to-know-to-not-be-dumb.

8. Joshua New, "Healthcare Insurance Regs Must Keep Up With Tech Advances," Center for Data Innovation, October 13, 2014, http://www.datainnovation.org/2014/10/healthcare-insurance-regs-must-keep-up-with-tech-advances/, Neil Versel, "Lively, a new eldercare monitoring system focused on social connections, heads to Kickstarter," Mobi Health News, April 16, 2013, http://mobihealthnews.com/21650/lively-a-new-eldercare-monitoring-system-focused-on-social-connections-heads-to-kickstarter/ and Dana Wollman, "The Internet of Toddlers: Inter Shows Off a Smart Baby Onesie," Engadget, January 7, 2014, http://www.engadget.com/2014/01/07/intel-smart-baby-onesie/.

9. Kira Newman, “The ‘Quantified Self’ Is Only the First Step to Better Health,” Tech Cocktail, May 28, 2013, http://tech.co/quantified-self-better-health-2013-05.

10. “Wireless Structural Monitoring System Deployed in Korea,” University of Illinois, November 30, 2009, http://cee.illinois.edu/node/1022.

11. “Smart Cities are Built on the Internet of Things,” Lopez Research, 2014, https://www.cisco.com/web/solutions/trends/iot/docs/smart_cities_are_built_on_iot_lopez_research.pdf.

12. Daniel Castro and Mark Doms, “Data is the Key to the Factory of the Future,” Center for Data Innovation, October 2, 2014, http://www.datainnovation.org/2014/10/data-is-the-key-to-the-factory-of-the-future/ and Udaya Shankar, “How the Internet of Things Impacts Supply Chains,” Inbound Logistics, 2014, http://www.inboundlogistics.com/cms/article/how-the-internet-of-things-impacts-supply-chains/.

13. “Finding Success in the New IoT Ecosystem: Market to Reach $3.04 Trillion and 30 Billion Connected ‘Things’ in 2020, IDC Says,” International Data Corporation, November 7, 2014, http://www.idc.com/getdoc.jsp?containerId=prUS25237214.

14. Peter C. Evans and Marco Annunziata, “Industrial Internet: Pushing the Boundaries of Minds and Machines,” General Electric, November 26, 2012, http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf.

15. Robert Atkinson, “ICT Innovation Policy In China: A Review,” Information Technology and innovation Foundation, July 2014, http://www2.itif.org/2014-china-ict.pdf.

16. Brian Heaton, “Internet of Things Helps Buffalo, Other Cities with Snow Removal,” Government Technology, November 19, 2014, http://www.govtech.com/data/Internet-of-Things-Helps-Buffalo-Other-Cities-with-Snow-Removal.html.

17. Jenni Spinner, “Headwall inks deal with USAFA on poultry inspection,” FoodProductionDaily.com, May 2, 2014, http://www.foodproductiondaily.com/Safety-Regulation/Headwall-inks-deal-with-USDA-on-poultry-inspection.

18. Jim Polson, “Water Losses in India Cut in Half by Smart Meters: Itron,” Bloomberg, March 15, 2013, http://www.bloomberg.com/news/2013-03-15/water-losses-in-india-cut-in-half-by-smart-meters-itron.html.

19. Alan McQuinn, “Commercial Done Companies Fly Away from FAA Regulations, Go Abroad,” Inside Sources, September 30, 2014, http://www.insidesources.com/commercial-drone-companies-fly-away-from-faa-regulations-go-abroad/.

20. Sandeep Rao, “Medical device approval plagued by unhealthy delays,” Baltimore Sun, February 24, 2011,

http://articles.baltimoresun.com/2011-02-24/news/bs-ed-fda-regulations-20110224_1_diseased-heart-valves-cardiology-fda.

21. Joshua New, "Will Obama be the Last Open Data President?," Center for Data Innovation, November 11, 2014, http://www.datainnovation.org/2014/11/will-obama-be-the-last-open-data-president/.

22. Brenna Berman, "2013 Open Data Annual Report," City of Chicago, 2013, http://report.cityofchicago.org/open-data-2013/.

23. Josh Taylor, "Chicago's smart city: From open data to rat control," ZD Net, October 15, 2014, http://www.zdnet.com/chicagos-smart-city-from-open-data-to-rat-control-7000034726/.

24. Daniel Castro, Ann Cavoukian, "Big Data and Innovation, Setting the Record Strati: De-identification Does Work," Information Technology and Innovation Foundation, June 16, 2014, http://www2.itif.org/2014-big-data-deidentification.pdf.

25. Nick Sinai and Matt Theall, "Expanded 'Green Button' Will Reach Federal Agencies and More American Energy Consumers," White House Office of Science and Technology Policy, December 5, 2014, http://www.whitehouse.gov/blog/2013/12/05/expanded-green-button-will-reach-federal-agencies-and-more-american-energy-consumers.

26. Daniel Castro, "The Rise of Data Poverty in America," Center for Data Innovation, September 10, 2014, http://www2.datainnovation.org/2014-data-poverty.pdf.

27. Alex Hern, "Google: 100,000 lives a year lost through fear of data-mining," June 26, 2014, http://www.theguardian.com/technology/2014/jun/26/google-healthcare-data-mining-larry-page.

28. "Smart Water: wireless sensor networks to detect floods and respond," Libelium, September 5, 2011, http://www.libelium.com/smart_water_wsn_flood_detection/.

29. Davey Alba, "This Wearable Detects Pollution to Build Air Quality Maps in Real Time," Wired, November 19, 2014, http://www.wired.com/2014/11/clarity-wearable and Martin LaMonica, "Greenbiz 10: What you need to know about the Internet of Things," GreenBiz, May 14, 2014, http://www.greenbiz.com/blog/2014/05/12/greenbiz-101-what-do-you-need-know-about-internet-things.

30. Daniel Castro and Travis Korte, "A Catalog of Every 'Harm' in the White House Big Data Report," Center for Data Innovation, July 15, 2014, http://www.datainnovation.org/2014/07/a-catalog-of-every-harm-in-the-white-house-big-data-report/.

31. Dan Keating, David Fallis, and Andras Petho, "ShotSpotter detection system documents 39,000 shooting incidents in the District," Washington

Post, November 2, 2013, http://www.washingtonpost.com/investigations/shotspotter-detection-system-documents-39000-shooting-incidents-in-the-district/2013/11/02/055f8e9c-2ab1-11e3-8ade-a1f23cda135e_story.html.

ABOUT THE AUTHORS

Daniel Castro is the director of the Center for Data Innovation where he leads the Center's research efforts. Mr. Castro is also a senior analyst at the Information Technology and Innovation Foundation. Previously, he worked as an IT analyst at the Government Accountability Office. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Joshua New is a policy analyst at the Center for Data Innovation. He has a background in government affairs, policy, and communication. Prior to joining the Center for Data Innovation, Joshua graduated from American University with degrees in C.L.E.G. (Communication, Legal Institutions, Economics, and Government) and Public Communication.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading think tank studying the intersection of data, technology, and public policy. Based in Washington, DC, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The Center is a non-profit, non-partisan research institute proudly affiliated with the Information Technology and Innovation Foundation.

contact: info@datainnovation.org

datainnovation.org

Unique Public-Private Partnership Targets IoT Security

By Dana Blouin | *Aug 31, 2015*

Anyone in the know knows the Internet of Things (IoT) is a hot topic these days.

The impact of the IoT is as wide as you can image, spanning everything from your toaster to your car to whole businesses and even cities. Everyone and everything seems eager to integrate the IoT in some way.

But many experts worry about IoT security and privacy — or the absence of security and privacy.

"Rapidly increasing incorporation of networked computation into everything from our homes to hospitals to transportation systems can dramatically increase the adverse consequences of poor cybersecurity," said Philip Levis, associate professor of computer science and electrical engineering at Stanford University.

Now the National Science Foundation (NSF) has teamed up with Intel to chip away at the problem.

Addressing an Issue

The NSF and Intel have formed an innovative cooperative research model.

They've created two new grants totaling $6 million, which will be directed at improving security for the Internet of Things. They're earmarked for teams that will study solutions to address Security and Privacy-Aware Cyber-Physical Systems and CPS-Security: End-to-End Security for the Internet of Things.

The inclusion of the NSF into the research behind the Internet of Things underscores the gravity of this topic.

The NSF, an independent US federal agency, supports fundamental research in science and engineering fields, with the exception of medicine.

This partnership between NSF and Intel represents a new model of cooperation between government, industry and academia that supporters claim will increase the relevance and impact of long-range research.

It can lead to better understanding and mitigation of threats "to our critical cyber-physical systems and secure the nation's economy, public safety and overall wellbeing," Jim Kurose, head of Computer and Information Science and Engineering at NSF, noted in a statement.

A Growing Concern

As the IoT grows, so will the problem.

Every day, IoT devices further integrate into our daily lives. We continue to share our data via our devices and leave a digital trail through our interactions.

This data holds great value for companies with the tools, technologies and strategies to analyze and act on it. However, it also creates risks for the end users.

Is anything really private anymore?

It's fair to say that most companies entering the IoT space are making data privacy a priority, for regulatory, legal and compliance issues alone.

And while defining privacy policies and taking steps to anonymize customer data is a good start, there's a lot more to be done.

As the amount of data we generate through our interactions increase, the necessity of IoT privacy and security will become even more paramount.

The Security Issue

Security for the IoT tends to focus on the connections between devices: the type of encryption being used and the ways the devices authenticate each other.

The IoT poses some very security challenges.

Many of the devices deal with significant power or processing constraints. What's more, many of the transitional communications protocols predate the IoT and the type of security it requires.

These kinds of issues make the NSF-Intel partnership grants a critical step forward.

While the IoT has advanced in spite of security and privacy issues, a single significant incident could stall its progress.

By stepping in and funding research, the NSF and Intel are jointly acknowledging that the IoT is more than a flash in the pan.

It could be the single most important technological change of our time.

Journal of Network and Computer Applications 35 (2012) 584–596

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

An overview of the Internet of Things for people with disabilities

Mari Carmen Domingo *

Electrical Engineering, UPC-Barcelona Tech University, Esteve Terradas, 7, 08860 Castelldefels (Barcelona), Spain

ARTICLE INFO

Article history:
Received 30 June 2011
Received in revised form
18 September 2011
Accepted 20 October 2011
Available online 29 October 2011

Keywords:
Internet of Things
People with disabilities
Architecture
Applications
Research challenges

ABSTRACT

Currently, over a billion people including children (or about 15% of the world's population) are estimated to be living with disability. The lack of support services can make handicapped people overly dependent on their families, which prevents them from being economically active and socially included. The Internet of Things can offer people with disabilities the assistance and support they need to achieve a good quality of life and allows them to participate in the social and economic life. In this paper, an overview of the Internet of Things for people with disabilities is provided. For this purpose, the proposed architecture of the Internet of Things is introduced. Different application scenarios are considered in order to illustrate the interaction of the components of the Internet of Things. Critical challenges have been identified and addressed.

Contents

1. Introduction . . . 584
2. IoT architecture . . . 585
   2.1. Perception layer . . . 585
      2.1.1. Visually impaired . . . 585
      2.1.2. Hearing impaired . . . 586
      2.1.3. Physically impaired . . . 586
   2.2. Network layer . . . 587
   2.3. Application layer . . . 588
3. Application scenarios . . . 589
   3.1. Shopping scenario . . . 589
   3.2. At school . . . 590
   3.3. Domestic environment . . . 592
4. Benefits of the IoT for disabled . . . 594
5. Research challenges . . . 594
6. Conclusion . . . 595
   Acknowledgments . . . 595
   References . . . 595

1. Introduction

The Internet of Things (IoT) is a technological revolution in computing and communications. It depicts a world of networked smart devices, where everything is interconnected (ITU Internet Reports, 2005) and has a digital entity (Pascual et al., 2011). Everyday objects transform into smart objects able to sense, interpret and react to the environment thanks to the combination of the Internet and emerging technologies such as Radio-frequency Identification (RFID) (Amaral et al., 2011), real-time localization and embedded sensors.

This technological evolution enables new ways of communication between people and things and between things themselves (Tan and Wang, 2010). In this paper, an overview of the IoT for people with disabilities is provided. The first ever World report on disability has been published in June 2011 (World Health Organization (WHO), 2011). Based on the 2010 population estimate (6.9 billion) and the 2004 disability prevalence estimate (World Health Survey and Global Burden of Disease), over a billion people including children (or about

* Tel.: +34 93 413 70 51.
E-mail address: cdomingo@entel.upc.edu

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.10.015

15% of the world's population) are estimated to be living with disability (World Health Organization (WHO), 2011). The report (World Health Organization (WHO), 2011) also revealed that 110 million people have very significant difficulties in functioning, while 190 million have "severe disability"—the equivalent of disability inferred for conditions such as quadriplegia, severe depression or blindness.

In addition, a recent study from the Organization for Economic Co-operation and Development (OCED) (2010) showed a huge labor market disadvantage. On average, the employment rate was 44% and 75% for people with and without disabilities, respectively. The inactivity rate was 49% and 20% for people with and without disabilities, respectively. Therefore, the inactivity rate for disabled people is about 2.5 times higher. Furthermore, the lack of support services such as building access, transportation, information and communication can make handicapped people overly dependent on their families, which prevents them from being economically active and socially included.

We strongly believe that the Internet of Things can offer people with disabilities the assistance and support they need to achieve a good quality of life and allows them to participate in the social and economic life. Assistive IoT technologies are powerful tools to increase independence and improve participation. Therefore, the purpose of this paper is to analyze how people with visual, hearing and physical impairments can interact with and benefit from the IoT. To the best of our knowledge, this is the first paper that discusses the IoT for handicapped people.

The paper is structured as follows. In the Section 2 we discuss the proposed architecture from a technical perspective. In Section 3, its application scenarios are described. In Section 4, the benefits of, and main research challenges to the IoT for handicapped are outlined in Section 5. Finally, the paper is concluded in Section 6.

2. IoT architecture

The proposed IoT architecture from a technical perspective is shown in Fig. 1. It is divided into three layers. The basic layer and their functionalities are summarized as follows:

- *Perception layer*: its main function is to identify objects and gather information. It is formed mainly by sensors and actuators, monitoring stations (such as cell phone, tablet PC, smart phone, PDA, etc.), nano-nodes, RFID tags and readers/writers.
- *Network layer*: it consists of a converged network made up of wired/wireless privately owned networks, Internet, network administration systems, etc. Its main function is to transmit information obtained from the perception layer.
- *Application layer*: it is a set of intelligent solutions that apply the IoT technology to satisfy the needs of the users.

Next, we describe in greater detail the components of each layer.

2.1. Perception layer

This layer provides context-aware information concerning the environment of disabled people. The components of this layer according to the disability of the person (visually impaired, hearing impaired or physically impaired) are described next.

2.1.1. Visually impaired

The components designed for the visually impaired are: (1) *body micro- and nano-sensors* and (2) *RFID-based assistive devices*. Next, those components are introduced.

2.1.1.1. Body micro- and nano-sensors. In Schwiebert et al. (2001), a *retinal prosthesis* is developed to restore some vision to patients affected by retinitis pigmentosa and age-related macular degeneration, two diseases that cause degenerative blindness. Although these disorders are characterized by the progressive loss of photoreceptor (rod and cone) cells of the outer retina, they do not affect the inner retinal ganglion nerve cells which form the optic nerve (Ye et al., 2010). Consequently, a camera mounted on a pair of glasses can be used to transmit image data to an implant attached to the retina, which is formed by an array of body micro-sensors. This artificial retina (Schwiebert et al., 2001) uses electrical impulses to stimulate the appropriate ganglion cells, which convert these electrical impulses into neurological signals. The generated response is carried via the optical nerve to the brain.

Currently, researchers are working to develop an *artificial retina at the nanoscale*. The venture Nano Retina is developing Bio-Retina, a bionic retina that incorporates several nano-sized components in a tiny retinal implant (see Fig. 2). Bio-Retina is designed to replace the damaged photoreceptor in the eye with the equivalent of a 5000 pixel (second generation) retinal implant. It transforms naturally received light into an electrical signal that stimulates the neurons, which send the images received by Bio-Retina

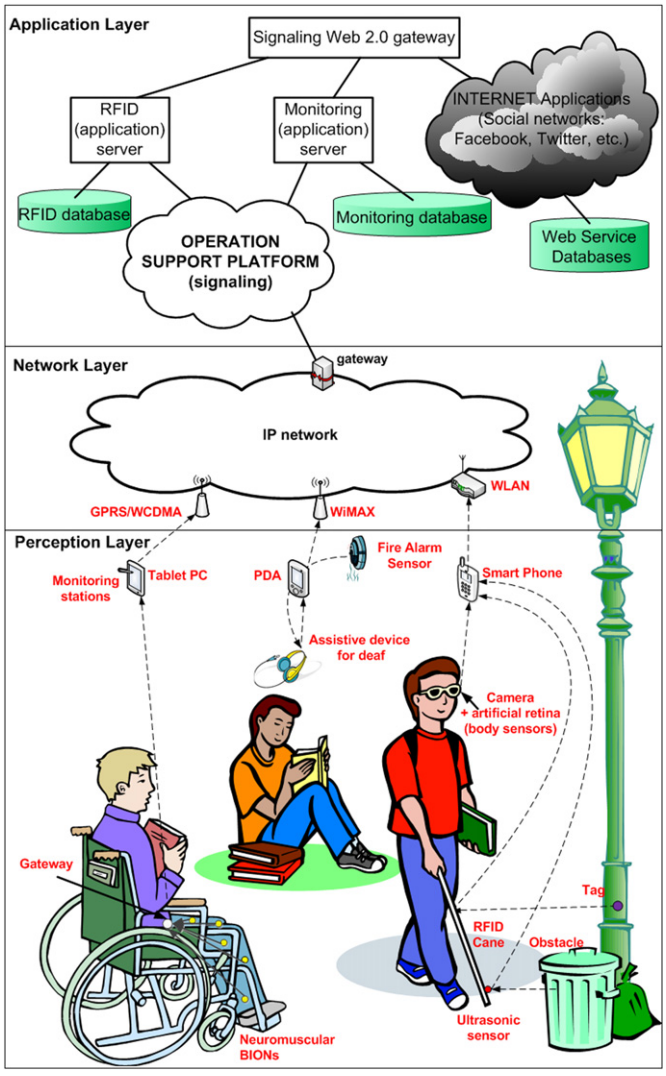


Fig. 1. Proposed architecture.

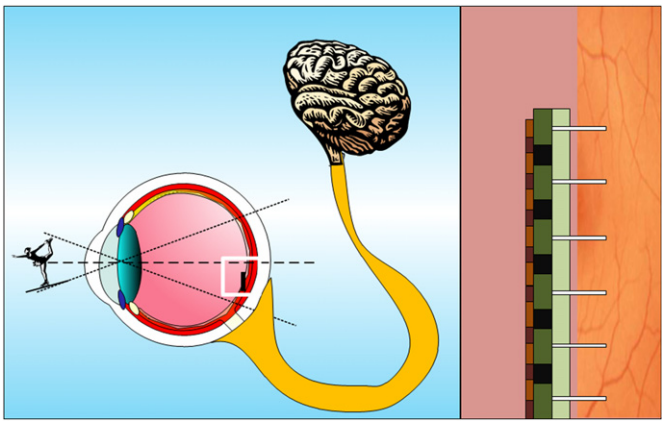


Fig. 2. Positioning of the retinal implant (left); bionic chip and its interface with the retina (right).

to the brain. The implant's nano-sized components are powered by a special pair of activation eyeglasses.

In the next years, as technology evolves, it will be possible to send information concerning the images captured by the artificial retina towards the monitoring station (smart phone) (see Fig. 1), so that new IoT applications to help people with visual impairments in their orientation, identification of faces, etc. will be developed.

2.1.1.2. RFID-based assistive devices. An essential RFID-based application is the *navigation system*. It helps blind people find their way in an unfamiliar area. RFID tags are distributed through the area. They can for example be placed in the center of the sidewalks to orient the blind person and prevent possible falls near the border of the sidewalk (Saaid et al., 2009).

The RFID cane (see Fig. 1) has a tag reader with an antenna that emits radio waves; the tags respond by sending back their stored data, hence identifying the location of the blind person. The tag reader (RFID cane) transmits via Bluetooth or ZigBee the data read from the RFID tag, which includes the tag ID string (D'Atri et al., 2007). This data is sent from the monitoring station through the network layer to the RFID server of the application layer. The blind person can record the destination's name as a voice message using the monitoring station. Directions are received by the monitoring station and played as voice messages (Shiizu et al., 2007).

An *obstacle detection system* based on an ultrasonic sensor can also be added (Martin et al., 2009). The sensor is mounted on the RFID cane to extend its effective range and perceive obstacles the cane alone would not be able to detect (such as a garbage can in Fig. 1). A voice message played at the monitoring station alerts the visually impaired when an obstacle is detected. A multiple sensor-based shoe-mounted sensor interface is also developed in Zhang et al. (2010) as a supplementary device to the cane to detect obstacles within 61 cm ahead of the visually impaired.

A widespread approach for outdoor navigation relies on Global Positioning System (GPS). It does not require tags to work. However, its resolution is limited (few meters) and it cannot work properly indoors. Therefore, some navigation systems for the visually impaired integrate both technologies (RFID and GPS) (Yelamarthi et al., 2010).

2.1.2. Hearing impaired

The components designed for the hearing impaired are: (1) *assistive devices and sensors* and (2) *RFID-based devices*. Next, those components are introduced.

2.1.2.1. Assistive devices and sensors. People who are hearing impaired can benefit from external or internal (implanted in the ear) assistive devices that improve hearing. Different types of sensors (such as doorbell or smoke detectors (see Fig. 1)) detect events or malfunctions that give rise to alarm conditions. Consequently, an alarm signal is sent from the sensors to the monitoring station, which forwards it to the assistive device as an amplified alarm signal. The deaf person can also be notified with visual (flashing light) or vibrotactile signals (vibration motor) (Ren et al., 2006).

On the other hand, HandTalk (Sarji, 2008) is a low-cost wireless glove designed to help the hearing impaired communicate with those who are not familiar with the American Sign Language (ASL). It recognizes basic ASL hand signs and converts them into voice by interfacing with a Java enabled monitoring station (cell phone or PDA). Basically, the glove is fitted with flex sensors (passive resistive devices that can be used to detect bending or flexing) along the fingers. The position (bending) of the fingers is sensed and sent to a monitoring station using Bluetooth. If the sensed data matches the set of values associated with an ASL sign of a cached database, the sign is converted into text and finally into speech.

2.1.2.2. RFID-based devices. RFID-tagged toys can be used to help deaf kids learn how to use sign language (see Section 3).

2.1.3. Physically impaired

The components designed for the physically impaired are: (1) *body sensors, actuators and neurochips* and (2) *body sensors and RFID technology*. Next, those components are introduced.

2.1.3.1. Body sensors, actuators and neurochips. Body sensors and actuators can be useful to perform functional reanimation of paralyzed limbs. Sensors attached to the nerves can detect the user's intention to move certain muscles and actuators can stimulate these muscles to restore the ability to move. A paralytic can be equipped with neuromuscular micro-implants named BIOnic Neurons (BIONs) (Tan and Loeb, 2007), which are modularly designed wireless capsules that can be injected at several sites in the body near motor nerves. Their main function is to reanimate paralyzed limbs. They receive power and digital command data from an external radio frequency coil and deliver stimulating current pulses to recruit the motor neurons and activate associated muscles. Sensors are required by the BION to detect voluntary command signals and to provide sensory feedback to regulate neuromuscular stimulation. This technology is used to create movements in limbs paralyzed by upper motor neuron disorders such as spinal cord injury and stroke. BIONs perform Functional Electrical Stimulation (FES), a technique that uses electrical currents to activate nerves innervating extremities affected by paralysis. This way, motor functions are recovered. Some examples of FES applications involve the use of neuroprostheses that allow people with paraplegia (Williamson and Andrews, 2000) to stand, walk, or restore hand grasp function in people with quadriplegia.

On the other hand, researchers at the Washington National Primate Research Center have deployed tiny, battery-powered implantable brain–computer interfaces (BCIs) (Fazel-Rezai, 2011) called neurochips in animals and are working on their implantation in humans.

When awake, the brain continuously governs the body's voluntary movements. This is largely done through the activity of nerve cells in the part of the brain called the motor cortex. These nerve cells, or neurons, send signals down to the spinal cord to control the contraction of certain muscles, like those in the arms and legs.

The neurochip records the activity of motor cortex cells. It can convert this activity into a stimulus that can be sent back to the brain, spinal cord, or muscle, and thereby set up an artificial

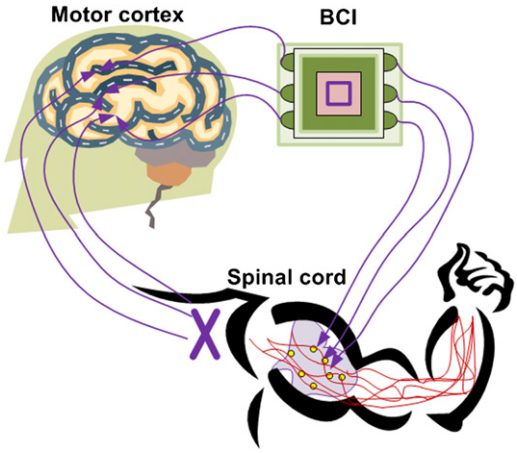


Fig. 3. BCI for spinal cord injury.

connection that operates continuously during normal behavior. This recurrent brain–computer interface creates an artificial motor pathway that the brain may learn to use to compensate for impaired pathways, as shown in Fig. 3. One potential clinical application is to bridge lost biological connections. Researchers have shown that monkeys can learn to bypass an anesthetic block in the nerves of the arm and to activate temporarily paralyzed muscles with activity of cortical neurons. BCIs are very promising in direct brain control of external devices. In Velliste et al. (2008), it is shown how primates restore self-feeding by controlling a 3-D robotical arm using their motor cortical activity. Another application is the promotion of neural plasticity to strengthen weak connections and rescue some impaired brain functions. It can help people move or speak again after a stroke or brain injury.

In addition, the company Berkeley Bionics has introduced eLEGS, an untethered exoskeleton, which allows wheelchair users to stand and walk. The exoskeletons are wearable, artificially intelligent bionic devices, which consist of a robotic frame controlled through crutches. The crutches contain sensors; putting forwards the right crutch moves the left leg, and vice versa.

2.1.3.2. Body sensors and RFID technology. Some paralyzed patients must wear a diaper when they are in bed. A wetness sensor can immediately alert nurses and caregivers to replace the diaper as soon as it becomes wet (Yang et al., 2008). The detected signal is sent towards a reader using an RFID reader.

2.2. Network layer

This layer (see Fig. 1) enables the access of the monitoring stations to the radio channel to transmit the information obtained from the perception layer. Although the Internet protocols were originally designed for fixed networks, there is a growing need for these protocols to accommodate mobile networks, as demonstrated by the use of many different wireless access technologies in IoT (EU FP7 Project CASAGRAS, 2009). The different transmission media include Wireless Local Area Networks (WLANs) (IEEE 802.11 variants), Worldwide Interoperability for Microwave Access (WiMAX) (IEEE 802.16), Bluetooth (IEEE 802.15.1), Ultra-wideband (UWB) (IEEE 802.15.4a and ECMA-368), ZigBee (IEEE 802.15.4), General Packet Radio Service (GPRS) and Wideband Code Division Multiple Access (WCDMA). Wireless ad hoc networks are a good option to establish wireless and mobile communications within the IoT, since they do not rely on a preexisting infrastructure, they require minimal configuration and are deployed quickly with low cost. Networks composed of different access technologies are known as *heterogeneous networks*

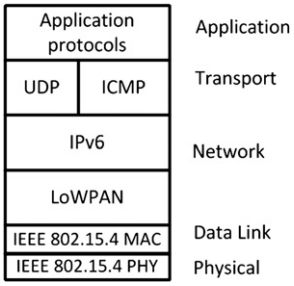


Fig. 4. 6LoWPAN protocol stack.

and they should maintain connectivity and service for different applications even with user mobility.

The convergence of heterogeneous networks and applications is possible due to the existence of a single Internet Protocol (IP)-based network. The IP for Smart Object (IPSO) Alliance is a non-profit association of more than 50 members from leading technology, communications and energy companies. They advocate the use of IP networked devices to build the IoT (Dunkels and Vasseur, 2010). They stress that IP is a long-lived and stable communication technology that supports a wide range of applications, devices and underlying communication technologies. In addition, the end-to-end IP architecture is lightweight, highly scalable and efficient. Furthermore, the authors of Internet Ø also recommend the use of the IP protocol to offer the Internet's interoperability and scalability directly to embedded devices rather than needing gateways for protocol conversion (Gershenfeld and Cohen, 2006).

It is necessary to ensure the connectivity, interoperability and compatibility of heterogeneous networks. The low-power networking industry, from ZigBee ad hoc control to industrial automation standards (e.g. ISA100), is quickly converging to the use of IP technology (Shelby and Bormann, 2009). In this sense, 6LoWPAN is the name of a working group of the Internet Engineering Task Force (IETF) that has developed a set of Internet standards, which enable the efficient use of IPv6 over Low-power Wireless Personal Area Networks (6LoWPANs). 6LoWPAN enables resource-limited embedded devices (often battery-powered) in low-power wireless networks to be Internet-connected by simplifying IPv6 (header compression of IPv6 header fields) and taking the nature of wireless networks into account.

The IPv6 protocol stack with 6LoWPAN is shown in Fig. 4. A small adaptation layer (named the LoWPAN adaptation layer) has been defined in the 6LoWPAN protocol stack (see Fig. 4) to optimize the transmission of IPv6 packets over IEEE 802.15.4 and similar link layers (Shelby and Bormann, 2009). IEEE 802.15.4 is a standard that defines the physical and MAC layers for low-power, low-rate wireless embedded radio communications at 2.4 GHz, 915 MHz and 868 MHz.

The adoption of Internet protocols by wireless embedded devices is challenging due to several reasons (Shelby and Bormann, 2009):

- Battery-powered wireless devices require low duty cycles, whereas IP is based on always connected devices.
- Multicast is not supported natively in IEEE 802.15.4 but it is essential in many IPv6 operations.
- Sometimes it is difficult to route traffic in multi-hop wireless mesh networks to achieve the required coverage and cost efficiency.
- Low power wireless networks have low bandwidth (20–250 kbit/s) and frame size (IEEE 802.15.4 packets are rather small, 127 bytes maximum at the physical layer, minus MAC/security and adaptation layer overhead). On the other

hand, the minimum datagram size that all hosts must be prepared to accept, for IPv6 is 1280 bytes. IPv6 requires that every link in the Internet has a Maximum Transmission Unit (MTU) of 1280 bytes or greater. On any link that cannot convey a 1280-byte packet in one piece, link-specific fragmentation and reassembly must be provided at a layer below IPv6.

- Standard protocols do not perform well in low-power wireless networks. For example, TCP performs very poorly in wireless networks due to its inability to distinguish between packet losses due to congestion and those due to channel error.

6LoWPAN is a group of Internet standards created to tackle all these problems. It implements a lightweight IPv6 stack adapted to low-power wireless devices and a Neighbor Discovery (ND) especially well-suited for low-power wireless mesh networks (Shelby and Bormann, 2009).

Routing and addressing are essential IoT networking issues. In Leal and Atzori (2009), scenarios where two or more gateways connect a Mobile Ad-hoc Network (MANET) of objects with the Internet (Multi-homed Hybrid MANETS) have been analyzed. A subnetwork is formed by MANET objects that share a common prefix announced by the closest gateway during address allocation. Gateway selection, dynamical address reallocation and routing changes when objects move from one subnetwork to another have been investigated. The network performance with respect to the packet delivery ratio, the end-to-end delay and the jitter with two different MANET routing protocols (AODV and OLSR) has been analyzed.

In addition, the IETF has developed an IPv6 routing protocol for Low power and Lossy Networks (LLNs) (including 6LoWPAN (Atzori et al., 2010)), that is, the RPL routing protocol (Clausen et al., 2011). LLNs are formed by smart objects with limited processing power, memory and energy (battery power). Unlike the MANET routing protocols, which perform well for ad hoc networks, RPL is optimized for upstream and downstream routing to/from a root node, a paradigm very appropriate for networks connected to the Internet. This routing protocol is essential for the deployment of IoT, since it enables traffic to be forwarded between low-power devices and the Internet. It has been designed assuming that the LLNs can comprise up to thousands of nodes and they are interconnected by unstable (lossy) links. The IETF Routing Over Low power and Lossy networks (ROLL) working group has defined application-specific routing requirements after focusing on a wide number of IoT applications: urban networks including smart grid, industrial automation, home and building automation. We also expect that this protocol is suitable for the IoT applications for handicapped people. Furthermore, RPL has been designed to operate over a variety of link layers such as IEEE 802.15.4.

RPL (Clausen et al., 2011) is a distance vector IPv6 routing protocol for LLNs. A Directed Acyclic Graph (DAG) is a graph having the property that all edges are oriented in such a way that no cycles (paths starting and ending on the same vertex) exist. All edges are contained in paths oriented toward and terminating at one or more root nodes (traditionally named sinks in Wireless Sensor Networks (WSNs)). RPL routes are optimized for traffic to or from one or more roots (sinks in WSNs). As a result, RPL uses the DAG topology and is partitioned into one or more Destination Oriented DAGS (DODAGs), one DODAG per sink. RPL specifies how to build the DODAG using an objective function and a set of routing metrics/constraints. The objective function computes the best path according to certain routing metrics and constraints. This way, DODAGs with different characteristics can be built. For example, different DODAGs are constructed with the objective to (1) find the best path in terms of link throughput (metric) while avoiding battery-operated nodes (constraint) or (2) find the best path in terms of latency (metric) while avoiding non-encrypted links (constraint). There could be several objective functions operating at the same node depending on the different path requirements of a given traffic. This way, it is possible to have multiple topologies (DODAGs) active at the same time to carry traffic with different requirements. The objective function also dictates some rules of the DODAG formation (number of parents, how to select them, load balancing, etc.). More details about RPL can be found in Clausen et al. (2011).

2.3. Application layer

This layer (see Fig. 1) provides an *operation support platform*, which can be accessed by monitoring stations and applications. It provides important functionalities such as authentication, billing, service management, service acceptance and routing of packets based on defined policies. IP Multimedia Subsystem (IMS) is a transport platform well-suited to perform these functions (Domingo, 2011), since services can be offered to the subscribers independently of the access media used, heterogeneous networks can be easily integrated and new applications and services can be rolled out faster reusing well defined common functions such as authentication, service provision, billing, group management and presence. This way, the IoT can be uniformly managed.

The Web of Things (WoT) is a vision where smart objects are integrated with the Web. Smart object applications can be built on top of Representational State Transfer (REST) architectures (Fielding and Taylor). The REST architectural style decouples applications from the services they provide, which can be shared and reused. The key abstractions of information in the REST architecture are resources (e.g. a document or image). Resources in web-based REST systems are identified by Universal Resource Identifiers (URIs). REST-style architectures consist of clients and servers. Clients initiate requests to servers; servers process these requests and return the appropriate responses. Resources are accessed by clients using methods such as GET, PUT, POST and DELETE of Hypertext Transfer Protocol (HTTP). The resources themselves are conceptually separate from the representations that are returned to the client. For example, the server does not send its database, but rather, perhaps, some HyperText Markup Language (HTML), Extensible Markup Language (XML) or JavaScript Object Notation (JSON) that represents some database records depending on the details of the request and the server implementation.

A web service is a software system designed to support interoperable machine-to-machine interaction over a network. Web services enable the communication between processes applying REST for the manipulation of resources using HTTP, or Simple Object Access Protocol (SOAP) for sending messages and making Remote Procedure Calls (RPCs) in a distributed environment.

However, the technologies deployed for web services are not appropriate for constrained networks and devices (Shelby, 2010). The protocols used to realize RESTful web services have several serious problems when applied to constrained networks. HTTP headers are frequently too large and require fragmentation in 6LoWPAN networks (using IEEE 802.15.4). TCP is not well-suited for wireless networks, the HTTP request/response pull model (request initiated by the client) does not work well in sensor networks with very low duty cycles and HTTP, as currently used between modern servers and browsers, has evolved into a highly complex protocol. Therefore, the RESTful web service paradigm needs to be extended.

The Internet Engineering Task Force (IETF) Constrained RESTful environments (CoRE) working group has defined a REST based web transfer protocol called Constrained Application Protocol

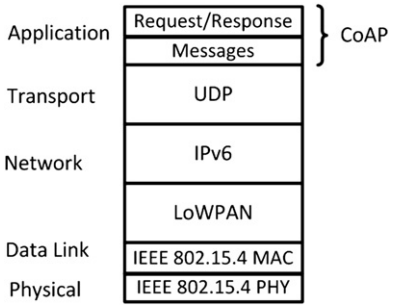


Fig. 5. CoAP protocol stack.

(CoAP) (Shelby et al., 2011). The aim of CoAP is to extend the REST architecture for constrained IoT devices and networks (e.g. 6LoWPAN). It has been designed taking into account the requirements of important Machine-to-Machine (M2M) applications such as energy and building automation. We also think it is appropriate for the IoT applications for people with disabilities. CoAP consists of a subset of REST common with HTTP functionalities, which have been optimized for M2M applications. CoAP offers features for M2M applications such as very low overhead, multicast support and asynchronous message exchanges.

The CoAP protocol stack is shown in Fig. 5. Unlike HTTP, CoAP exchanges messages asynchronously over a datagram-oriented transport protocol such as User Datagram Protocol (UDP). TCP is not well-suited due to its bad performance in LLNs, sensitivity to mobility, no multicast support and high overhead for short-lived transactions (Shelby, 2010). Since CoAP is built on top of UDP, its overhead is lower and it supports efficient IP multicast. Since UDP is non-reliable, CoAP implements a lightweight reliability mechanism, without trying to re-create the full feature set of TCP.

CoAP is divided into two layers (Shelby et al., 2011): the messaging and the request/response layer. The messaging layer deals with the asynchronous exchange of messages over UDP between end-points. There are four different types of messages: Confirmable (CON) (these messages require an Acknowledgment (ACK)), Non-confirmable (NON) (they do not require an ACK), Acknowledgment (ACK) (they acknowledge a confirmable message) and Reset (RST) messages (they indicate that a confirmable message was received, but some context is missing to properly process them). The Request/Response layer handles the transmission of requests and responses for resource manipulation and transmission. A request is carried in a Confirmable (CON) or Non-confirmable (NON) message. The response to a request in a CON message is carried in the resulting ACK message. The reliability mechanism consists of a simple stop-and-wait retransmission protocol with exponential back-off for ''confirmable'' messages between retransmissions. It detects both ''confirmable'' and ''non-confirmable'' duplicates and it supports multicast.

CoAP uses a short fixed-length header (4 bytes) that may be followed by options (e.g. URI and payload content-type) and a payload. This way, the overhead is significantly lower than in HTTP with the purpose of limiting fragmentation.

In the application layer the services are run by application servers, which host and execute the services and provide the interface to communicate with the operation support platform. We have identified some important application servers in the IoT for people with disabilities (see Fig. 1). The *RFID application server* is useful in the *navigation system for blind* application. It receives tag information concerning the current location and destination of the blind person. The best route is computed using the shortest path algorithm. When a user is lost, the tags in the way help to detect it and a new route towards the destination is computed based on the current location. This route is sent back to the monitoring station using the IP network. The RFID database stores and updates data concerning the user, his/her path achievement, destination changes and path preferences.

The *monitoring application server* offers application codes (such as Ajax) to process the sensed data the disabled person/professionals wish to control. Periodic reports and visual graphs are sent to the monitoring station of the user. The sensor nodes transmit the sensed data via web services according to the disability and/or preferences of the user. For instance, the doctor of a paralytic might want to control periodically the state of the BION sensors or a nurse the wetness sensor data of diapers; a deaf person might be interesting in reviewing the alarm reports of his/her smart home.

The signaling Web 2.0 gateway (see Fig. 1) interconnects the transport platform and the Web 2.0 domains. People with disabilities can access Internet to search for real-time information (e.g. location of an open restaurant or a free parking lot for handicapped) or to keep contact with relatives/friends using social networks.

3. Application scenarios

Next, several application scenarios of the Internet of Things for handicapped people are introduced. They illustrate the interaction of the different components of the IoT architecture.

3.1. Shopping scenario

In this scenario, people with visual impairments shop autonomously as shown in Fig. 6. The *blind navigation system* helps them to find their way in a store. The store's RFID system can use software to guide the visually impaired in shopping. In López-de-Ipiña et al. (2011), an RFID-tag based navigation system is proposed. The supermarket is divided into cells containing a shelf and passageway cells. RFID tags are distributed through the floor. The tag IDs within a cell are mapped to navigation information such as the type of a given cell and the types of neighboring cells. The monitoring station (smart phone) maintains a Bluetooth connection with the RFID reader (smart cane) of the user to keep track of his/her position anytime using the mapping of tag IDs with navigation information. The speech synthesis and recognition module of the monitoring station (smart phone) enables the visually impaired person to say the section of the supermarket where he/she wants to go. The route to follow is obtained invoking web services through a WLAN connected to the Internet. As the visually impaired walks, routing directions from an android application are received through the headphone of the smart phone and played as voice messages.

RFID tags attached to the supermarket products supply product data such as name, description and price. Sensor enabled RFID tags provide essential data such as temperature or shocks during transportation. The tag reader (RFID cane) transmits the tag ID string to the monitoring station, which forwards it to the RFID server (Krishna et al., 2008). Product information is returned from the RFID database to the monitoring station and played as voice messages. Additional product characteristics can include food composition, caloric intake and specific data related to the user profile such as food allergies and intolerances. Friend's opinions about the product and price comparison with similar ones can be obtained using social networks. In Krishna et al. (2008), experiments of the RFID system were conducted to study detection range of RFID readers with respect to different tags and materials (where the tag is installed); it was concluded that the

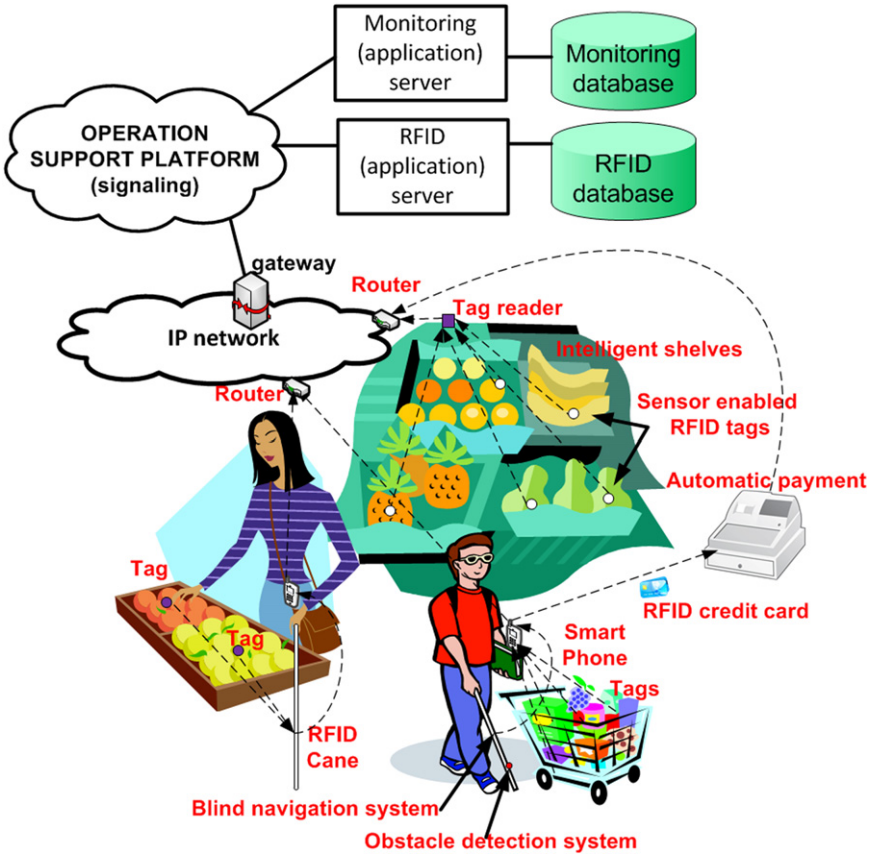


Fig. 6. Shopping scenario.

product materials did not affect the performance of the RFID readers.

Several practical works have been developed related to this application scenario (Kulyukin and Kutiyanawala, 2010; Lanigan et al., 2007; Narasimhan, 2006; Nicholson et al., 2009; Winlock et al., 2010). In Lanigan et al. (2007) the authors propose Trinetra, a system designed to assist blind people in grocery shopping for product search and identification. As the visually impaired scans a grocery item with a portable barcode or RFID reader, the scanned input is sent via Bluetooth to the user's smart phone, which checks its cache for a product match. In case of cache miss, the smart phone communicates through GPRS with a remote server or, in case of miss, with a public Universal Product Code (UPC) or RFID database, which converts the barcode or tag into a human-interpretable product name (and related information) and returns it to the smart phone. An onboard text-to-speech software in the smart phone converts the displayed text into speech. The advantages of RFID tags compared to barcodes are reprogrammability, ability to contain more product information and ability to read without line-of-sight reading (Narasimhan, 2006). Trinetra was successfully tested at the Carnegie Mellon University's campus store.

ShopTalk (Nicholson et al., 2009) is a wearable system to assist visually impaired shoppers. The users get verbal instructions from a handheld computer. Modified Plessey (MSI) barcodes located on the shelves enable navigation within the store. UPC barcodes enable product localization in a store aisle. In a production version, the system would connect to the store's inventory control database and look up product information. Successful experiments with visually impaired participants were performed at supermarkets.

GroZi (Winlock et al., 2010) focuses on real-time product detection from mobile video in grocery stores. A user compiles a shopping list of products on the website and uploads it on a portable device. Later, the shopper scans a scene in the supermarket with a camera. GroZi uses in vitro images of items (images of products taken under ideal lighting and perspective conditions) on the user's shopping list to detect items in situ (from actual video stream). A hand glove with vibrating motors and the audio of the portable device are used to guide the shopper. The capability of detecting a shopping list's items is demonstrated with experiments.

Automatic payment can also be performed using RFID. A scanner reads all items in the cart at once, totals them up and charges the customer's account while adjusting the inventory. RFID credit cards use a radio frequency to transmit personal financial data.

Furthermore, periodic reports and statistics concerning the shopping can be computed and sent periodically from the monitoring server to the monitoring station.

3.2. At school

The school scenario is shown in Fig. 7. The authors in Hengeveld et al. (2009) show the great added value of designing intelligent interactive play and learning environments for toddlers (from one and half to four years old) with multiple disabilities to stimulate their language and communication skills. These play and learning systems include RFID technology to identify different materials (such as a child's toy sheep). On the other hand, RFID-tagged toys are used to help deaf kids ages three to four learn how to use sign language (Parton et al., 2010). The software developed enables a child to use a RFID reader to scan an item's tag, capture the unique identifying number and send it to the computer's software via the USB connection. An animation is launched, which includes videos of a person and of an avatar

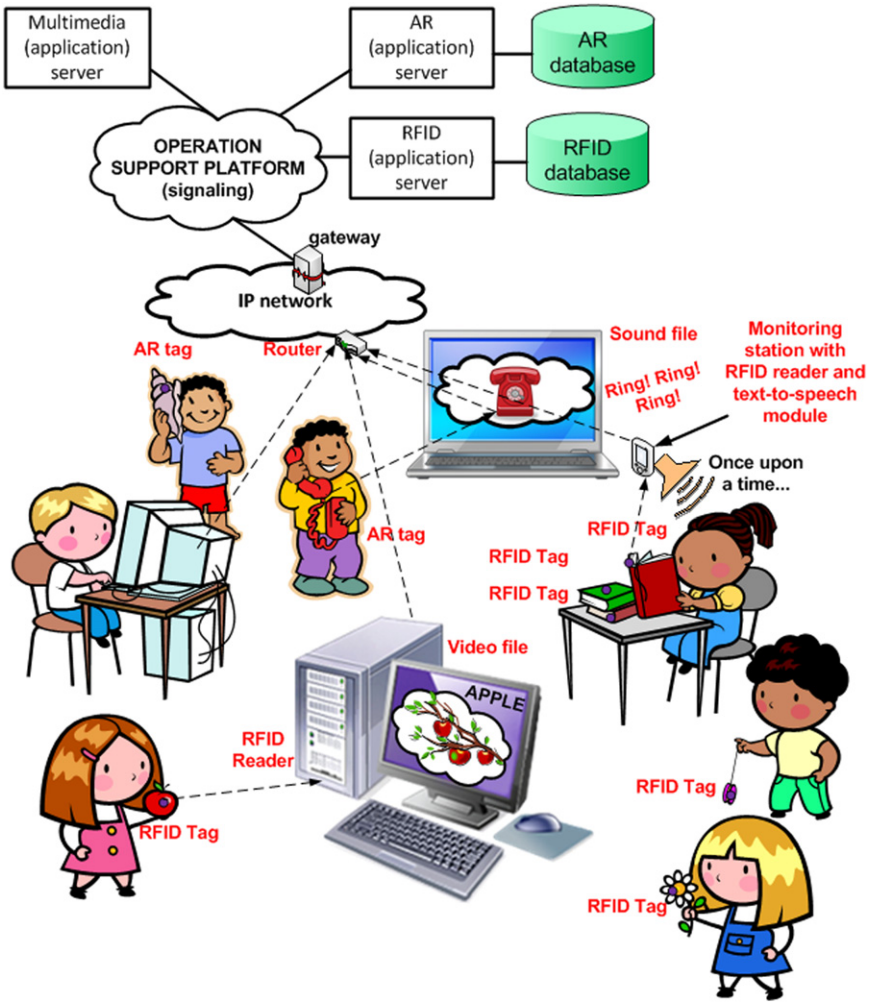


Fig. 7. School scenario.

signing that item (in American Sign Language (ASL)) as well as several pictures of the item to familiarize the child with the many versions of the object (e.g. multiple types of ships). The concept is also shown in written English for a bilingual approach to language acquisition. The system was integrated into the early childhood curriculum at the Louisiana School for the Deaf for four weeks to determine its impact on vocabulary acquisition, and the results were positive (Parton et al., 2009). In addition, the authors in Parton et al. (2010) concluded that low cost RFID tags/readers were more appropriate than low cost barcode reader/tags for this educational setting (tested with K-6 students in elementary school), since 99% of the students were able to launch the animations successfully with the RFID reader/tag and only 26% with the barcode reader/tag. Furthermore, success was obtained with RFID technology instantly (1–15 s to successfully scan) in 96% of the launched animations. Currently, information concerning the tagged objects is stored on a computer. However, the application could be managed more efficiently using a RFID server and database; the multimedia videos could also be stored and downloaded by an application server. We also suggest that more than one object could be scanned at the same time by the tag reader to establish associations between different objects and their nouns. In this case, a new multimedia video would be launched signing and including examples of the objects altogether. In addition, single-microchip tags could be attached to the same object (RFID grid). For instance, a doll with tags attached at different body parts could be scanned by the reader to launch different instructive videos. This way, children could learn to identify the different body parts.

We also propose to go one step further and extend this technology to zoo or farm visits where children with tag readers and monitoring stations could learn concepts looking at real things (true apple or elephant instead of plastic ones). The tag reader would communicate to the monitoring station the tag ID string of the scanned object, which would forward this information to the RFID server. Information concerning the scanned object is returned from the RFID database to the monitoring station and a multimedia video would be played.

Augmented Reality (AR) combines real world and computer generated scenes. Its major components are tags, a web-cam and image processing devices. A program is launched on a computer to recognize real AR objects. This program is able to obtain the tag ID from real AR objects and locate them in a database. It is possible to watch the objects on the screen, launch a sound file in real-time, etc. For instance, a picture card can contain an AR tag. The AR image processing device recognizes the picture card when it appears on screen and uses the tag to identify the picture card type. The corresponding sound (e.g. a telephone ringing) is then introduced to realize the merging of virtual sound with real imagery (Chien-Yu et al., 2010). This way, sensory or mentally handicapped children can learn common everyday sounds. Using the feel of different material supplemented by audio explanations allows visually impaired children to learn about different

materials and experience them through their sense of touch (Chien-Yu et al., 2010). Studies (Chien-Yu et al., 2010) with physically challenged children from kindergarten to first grade demonstrated that AR is a highly effective assistive technology. Other AR applications allow children to handle 2D and 3D plant entities (fruits, flowers, leaves, seeds) (Richard et al., 2007). They should reach for and handle a given entity (located on a tangible marker) and position it at the location instructed by the AR system. Visual (entities surrounded by a red/blue circle are wrong/right positioned), auditory (names of the entities are played using audio) or olfactory (odor of the entity) cues are provided to help them in decision-making.

In addition, children with visual impairments can locate specific books using RFID technology and 'read' them using the text-to-speech module of a monitoring station (see Fig. 7). In Parton and Hancock (2011), ongoing research on the use of RFID embedded storybooks with deaf children is presented. Videos depicting a story in ASL are launched in a computer every time the deaf children scan the tags of the book pages. The study conducted with a prototype was very successful, and both teachers and deaf students showed very positive reactions.

3.3. Domestic environment

Smart home technology (see Fig. 8) refers to the integration of technology and services through home networking for a better quality of living. Smart homes enable the *automation and control of the home environment* using multiple devices such as automatic kitchen equipment, light and door controllers, indoor temperature controllers, water temperature controllers and home security devices (Stefanov et al., 2004). These *home devices for automation and control* are formed by sensors and actuators embedded in goods, home appliances or furniture. The sensors monitor the environmental conditions, process collected information and cooperate with other

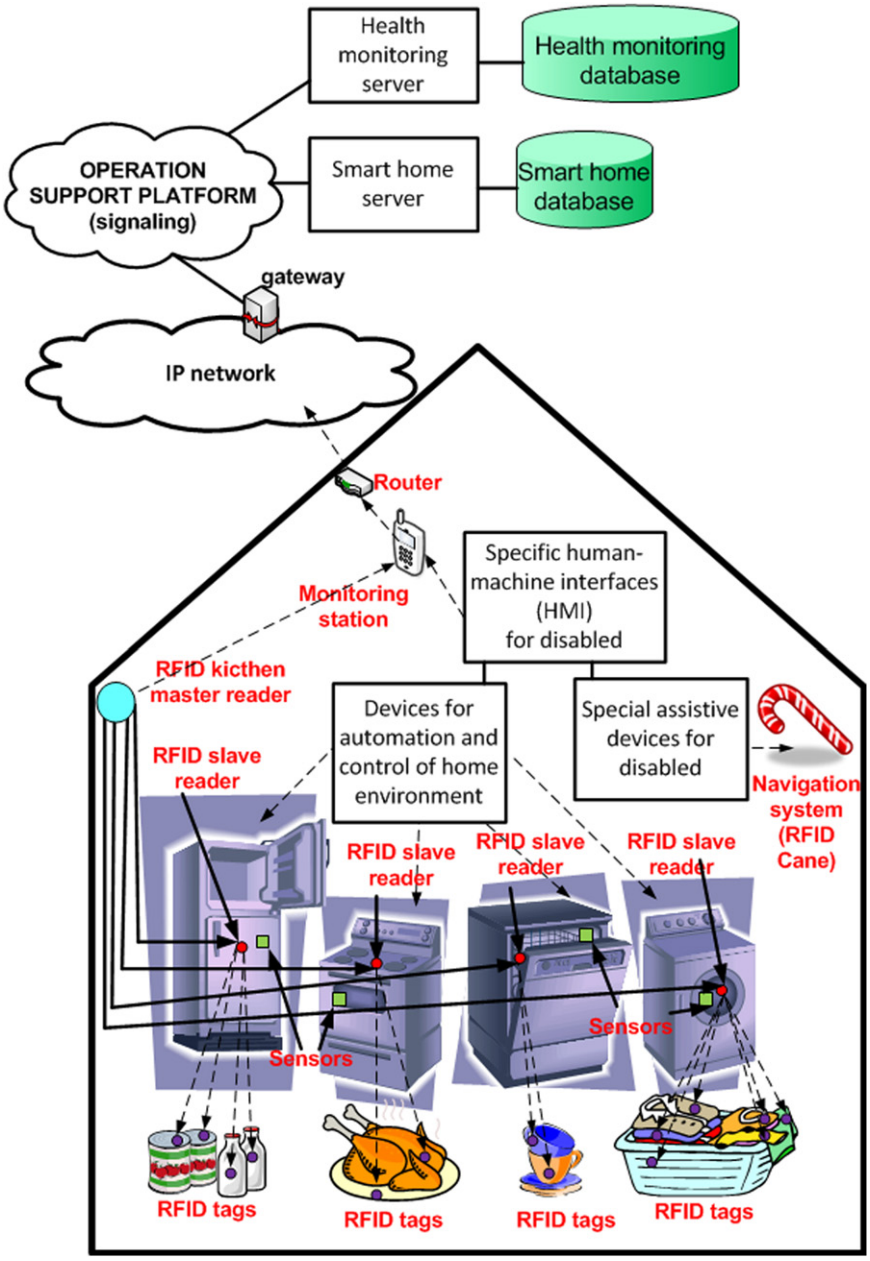


Fig. 8. Smart home scenario.

units through a wireless network. The collected information is then processed by a server to provide suitable services to the user. If events that give rise to alarm conditions are detected, actuators are triggered for handling the current emergency situation (e.g. burglar or fire alarm).

The integration of RFID in the smart home environment is also essential for identification and tracking purposes. In Darianian and Michael (2008), a master–slave RFID architecture is proposed. Slave readers integrated in the home appliances communicate with mobile readers (monitoring stations) and a master reader, which is connected to a smart home server. Different master readers can communicate with each other and the mobile readers. This system is applied to home washing control as shown in Fig. 8. RFID tags attached to clothes contain information about color, material and suitable washing program. If the amount of dirty clothes detected by a RFID reader reaches a threshold, an alarm is automatically sent and an energy-aware washing program is suggested. The reader also checks the compatibility between clothes when the washing machine is being loaded. The dirty clothes left for the next washing are also monitored with the aid of the smart home server and a database. Other smart home applications combine Internet services with RFID identification. The slave readers in the fridge and shelves communicate to a master reader in the kitchen to suggest cooking recipes based on the resident's preference and his/her health conditions (food allergies or cholesterol), invoking web services that supply recipe search and download. The health monitoring server and database are useful to monitor and record the health conditions of the resident. The smart home server and database are also useful to record the resident's list of required food items and the current availability of these items to compare them and generate a shopping list automatically.

Furthermore, an automation logic is proposed in Buckl et al. (2009) to optimize the power consumption throughout the day, According to the price of electricity obtained from an external web service, the energy consumption in the house is diminished (e.g. disconnecting the house from the power grid and using energy from a battery, putting the refrigerator in an energy saving mode until a temperature threshold is met, etc.). A future home automation scenario is developed in Buckl et al. (2009) for demonstration purposes.

Modern sensor-embedded houses or smart houses can assist impaired people and resolve their social isolation (Chan et al., 2008). Smart homes are adapted to people with disabilities in two different ways: (1) *specific interfaces* are designed to manipulate *the home devices for automation and control* and (2) *special assistive devices* are specifically designed to improve their living conditions at home.

The *specific interfaces* required to assist disabled people in the control of smart homes are summarized as follows (Stefanov et al., 2004):

Visually impaired people require:

- Specialized Human Machine Interface (HMI): it refers to the operational subsystem to control home equipment (lamps, TV sets, doors, etc.). Specialized zooming devices (both optical and optoelectronic) allow people with low vision to control the home environment. A retinal prosthesis (Schwiebert et al., 2001) can also enhance their vision (see Section 2.1.1). Voice control of home-installed devices is also a proper method.

Hearing impaired people require:

- Specialized HMI: touch screens to access graphical information and read text. Assistive devices for deaf are helpful (see Section 2.1.2).

Physically impaired people require:

- Specialized HMI: people affected by serious paralysis can use head-tracking devices to produce up to three independent proportional signals (forward–backward head tilting, left–right head rotation and lateral head tilting). Other techniques involve facial detection, eye-movement control, brain control, gesture recognition and facial expression recognition. In Sun Ju et al. (2009), an intelligent wheelchair is proposed; it determines its direction based on the inclination of the user's face and is stopped depending of the shape of the user's mouth.

Some examples of *special assistive devices* required to assist disabled people in improving their living conditions at home are summarized as follows:

Visually impaired people require:

- Devices for indoor navigation: a navigation system (Saaid et al., 2009) and an *obstacle detection system* (Martin et al., 2009) based on voice-synthesized instructions are valuable (see Section 2.1.1).

Physically impaired people require:

- Electro-mechanical devices for movement assistance: typical devices include powered wheelchairs and specialized lifting devices to transfer the user between the bed and the wheelchair. In Ahmad and Tokhi (2011), a two-wheeled wheelchair able to lift the front wheels (casters) to achieve an upright position has been designed. This way, the disabled persons who cannot stand on their own can reach certain heights and are able to pick and place things on shelves.
- Robotic systems for movement assistance: rehabilitation robots are designed to assist individuals in their everyday needs, such as eating, object replacement, etc. In Satoh et al. (2009), a method for bathing care assistance using the robot suit HAL is introduced.

These special assistive devices can also include specific Human Machine Interfaces (HMIs) (if necessary) to allow handicapped people to control them.

An important RFID-based application especially useful to provide a better quality of life for visually impaired people at home is a *search engine* to find objects (Welbourne et al., 2009). Personal objects are labeled with RFID tags. Metadata containing object-related data is created such as name, type, image URL or last registered location. Sensory context information (such as temperature) can also be acquired with the aid of sensors. All this information is introduced and managed with a web-based tool. This way, physical objects are linked to virtual ones. Different RFID readers are set at specific home locations. Another web-based tool is used to specify how to transform a user's tag-read event into high-level information. Labels such as 'with', 'without', 'near', 'far', 'inside' and 'outside' help to link tagged objects with people, places and events. For instance, a RFID reader can register the user leaving the house 'with' the wallet. This way, the last recorded location of a tagged object can be found. Users can be notified when they leave home 'without' a particular item (with a voice-synthesized message if they are visually impaired people). A four-week study was successfully conducted to measure trends in utilization of the designed RFID tools and applications as well as users' qualitative reactions. A different RFID reminder tool has been developed in Hsu et al. (2011). It compares the objects taken by the user when he/she leaves home with an object list generated by the system based on a calendar and the user's activities. The application sends a warning message to the PDA of

the user when he/she leaves home and one or more objects theoretically needed are missing. Experiments were successfully carried out with a prototype of the system.

4. Benefits of the IoT for disabled

Environments can foster the participation and inclusion of disabled individuals in social, economic, political and cultural life (World Health Organization (WHO), 2011). The IoT creates enabling environments by offering people with disabilities assistance in building access, transportation, information and communication.

Next, the benefits of the IoT for handicapped people are discussed. We focus on the benefits of applying the IoT in the application scenarios described in the previous section.

The IoT applied to smart homes or shopping scenarios makes it easy for people with impairments to carry out their daily activities. This increases their autonomy and self-confidence. Being independent in one's daily activities without requiring assistance from a sighted person is the highest priority for the visually impaired (Lanigan et al., 2007); applying IoT to shop autonomously fulfills these needs. In addition, smart homes offer disabled people independence in mobility, object manipulation and human–machine interfaces (HMIs) for communication. Home automation carries out certain daily activities (e.g. lighting control) automatically for them. Furthermore, monitoring systems improve the autonomy of handicapped people at home, since they reduce or eliminate control visits of caregivers.

On the other hand, sensory or mentally handicapped children can use interactive play and learning IoT environments ('at school' scenario) to experience a richer learning experience (cognitive skill development), have more opportunities for language acquisition (linguistic skills), become better at interacting with others (social skill development) and thus obtain higher self-esteem (emotional skill development) (Hengeveld et al., 2009). In addition, these interactive IoT systems adapt to their learning rhythm. For instance, deaf children often need additional exposure to the American Sign Language because most on their parents are hearing and not fluent in this language (Parton et al., 2009). Now they can take this interactive IoT system with them from school to home and repeat the most difficult vocabulary until they understand and memorize it. Learning is less difficult with this innovative and friendly system (it turns into a game) and learning barriers are reduced. This fact is especially important, since there is a strong correlation between early signed language exposure for deaf children and later academic achievement (Parton et al., 2009).

5. Research challenges

Next, the research challenges to IoT for people with disabilities are introduced.

A key challenge *is customization for people with disabilities*. Since handicapped people have special needs, the IoT should be adapted to their particular circumstances. Smart workflows are context-aware processes that are executed pervasively. They take context-aware decisions based on context information of the environment captured automatically by sensors. The authors in Wieland et al. (2008) describe an architecture that converts low-level context-aware information captured by sensors into information at the business level using smart workflows. Developers use business process modeling tools to describe smart workflow tasks. Presto is a model-based (Giner et al., 2010) software architecture that captures the concepts that are involved in the interaction between physical elements and their digital counterparts. When the business models are deployed in an execution engine, humans are usually required to perform some tasks in a workflow. Presto's architecture processes these demands and offers the appropriate mechanisms for users to complete these tasks by enabling their interaction with the physical world. The resulting system is capable of presenting to each participant in the process the services associated with his/her context (physical environment) according to his/her role and current pending tasks. This way, the user is guided through a workflow. For example, if a library member with a monitoring station (PDA) enters the library, Presto shows in the monitoring station the tasks that the user can initiate and complete depending on the available task processors. We propose that if the user is disabled, the list of tasks is received in an appropriate way. For instance, the return boxes of the library automatically detect the returned books by means of RFID. If the disabled person selects the 'return book' option, different ways to orient the user towards the closest return box according to his/her disability should be provided (visual or auditory related information, indications for paralytics about how to access the area where the return box is, etc.).

Another significant challenge to the IoT for people with disabilities is *self-management*. It refers to the process by which the IoT manages its own operation without human intervention. For this purpose, support for *self-configuration*, *self-healing*, *self-optimization* and *self-protection* capabilities is required (Haller et al., 2009). Self-configuration is related to the automatic configuration of components; self-healing handles the automatic discovery and correction of faults; self-optimization focuses on the automatic monitoring and control of resources to ensure the optimal functioning with respect to the defined requirements; self-protection tackles the proactive identification and protection from arbitrary attacks. Self-healing is particularly important, since handicapped people usually depend on IoT devices to compensate for their disabilities. Therefore, the detection and elimination of faulty nodes and the design of efficient fault-tolerant algorithms are required.

Standardization is also a very important challenge. It is necessary to create globally accepted standards to avoid *interoperability* problems. 6LoWPAN provides wireless internet connectivity to low-power devices with limited processing capabilities, so that they can be used in the IoT. As a result, with this standard, interoperability and integration with current heterogeneous Internet-aware devices is accomplished to expand the IoT for disabled people. On the other hand, existing mobility protocols like Mobile IP for IPv6 (MIPv6) or management protocols like Simple Network Management Protocol (SNMP) cannot be directly applied to 6LoWPAN devices, since they are inefficient in terms of energy, communication and computation cost (Jara et al., 2010). Therefore, more research to adapt existing protocols or find new solutions is required.

Furthermore, enabling people with disabilities to establish deeper contact with the outside world is challenging. IoT objects can automatically share pictures, comments and sensor data via social networks. For instance, relatives of a disabled person that belong to the same social network can obtain real-time data about the activities of the handicapped person (if he/she is sleeping, eating, leaving home, has fallen, etc.). This information is automatically sent by 'smart objects' that surround the disabled person in his/her domestic environment (smart home) (Kranz et al., 2010). Although direct communication with devices via social networks seems to be an exciting and promising way of maintaining social contact, the possibility of *machines flooding social networks* with auto-generated content exists.

The amount of traffic in the IoT will rise exponentially once connections between most objects are established in the next

years. *Scalability* is required to guarantee the proper functioning of the IoT with a very high number of nodes. Senseless communications between 'things' should be avoided to favor scalability, since they increase the communication overhead and energy consumption. However, a minimum number of connections between devices should be established for the proper functioning of applications (such as enough tag density and messages to orient a blind person).

In addition, *security and privacy issues* are real (Zorzi et al., 2010). It is essential to guarantee the privacy of the IoT for people with disabilities, who are particularly vulnerable. The IoT should be protected against distributed denial-of-service attacks, which can be defined as the result of any action that prevents any part of the IoT from functioning correctly or in a timely manner. The vulnerabilities of applications and sensors are exploited to launch such attacks. Consequently, an efficient security framework should be developed.

Cooperation between devices in the IoT is also indispensable (Zorzi et al., 2010). Scenarios where more capable nodes (monitoring stations) discover other resource-restricted nodes, synchronize with one another and help each other in reliable data delivery seem very promising. Nowadays, most IoT mass consumer applications are mobile devices-centered, since monitoring stations are more likely to integrate sensing, computing and communication capabilities. However, we envision that over time more direct thing-to-thing connections (between 'things' that are currently considered resource-restricted) will be established as communication, processing capabilities, technologies deployed for web services and energy harvesting techniques evolve.

Finally, we envision that the IoT for disabled people (especially physically disabled individuals) will evolve dramatically in the following years. The advances of brain–computer interfaces (BCIs) made possible the development of prototypes such as brain-controlled prosthetic devices, wheelchairs, keyboards and computer games. In the following years BCI technologies will be brought out of the lab and transform into real-world applications (Millán et al., 2010). Disabled people will benefit from the *advancements in BCI technology combined with assistive technologies* in four basic application areas (Millán et al., 2010): communication and control (Internet browsing, e-mails), motor substitution (in particular grasping and assistive mobility), entertainment (gaming, music browsing, photo browsing and virtual reality) and motor recovery. Neurophysiological signals (electroencephalogram, EEG) originating from the brain will be used to control external devices (e.g. TV, phone, computer, bed), which means human beings will be fully embedded in the Internet of the Things.

6. Conclusion

In this paper, an overview of the IoT for people with disabilities is provided. The relevant application scenarios and main benefits have been described. The research challenges have also been surveyed. These research issues remain wide open for future investigation.

Acknowledgments

This research work was supported by the Spanish Ministry of Science and Innovation under the project TIN2010-20136-C03-01.

References

Ahmad S, Tokhi MO. Linear quadratic regulator (LQR) approach for lifting and stabilizing of two-wheeled wheelchair. In: Proceedings of the fourth international conference on mechatronics (ICOM); May 2011.

Amaral LA, Hessel FP, Bezerra EA, Corrêa JC, Longhi OB, Dias TFO. eCloudRFID—a mobile software framework architecture for pervasive RFID-based applications, vol. 34(3); 2011. p. 972–9.

Atzori L, Iera A, Morabito G. The internet of things: a survey. Computer Networks 2010;54(15):2787–805.

Berkeley Bionics. 〈http://berkeleybionics.com/exoskeletons-rehab-mobility/〉.

Buckl C, Sommer S, Scholz A, Knoll A, Kemper A, Heuer J et al. Services to the field: an approach for resource constrained sensor/actor networks. In: Proceedings of the international conference on advanced information networking and applications workshops (WAINA '09); May 2009.

Chan M, Estève D, Escriba C, Campo E. A review of smart homes—present state and future challenges. Computer Methods and Programs in Biomedicine 2008;91:55–81.

Chien-Yu L, Chao J-T, Wei H-S. Augmented reality-based assistive technology for handicapped children. In: Proceedings of the international symposium on computer communication control and automation (3CA); May 2010.

Clausen T, Hui J, Kelsey R, Levis P, Pister K, Struik R, Brandt A, et al. In: Winter T, Thubert P, editors. RPL: IPv6 routing protocol for low power and lossy networks. Internet draft. draft-ietf-roll-rpl-19; March 2011 [work in progress].

Darianian M, Michael MP. Smart home mobile RFID-based internet-of-things systems and services. In: Proceedings of the international conference on advanced computer theory and engineering (ICACTE '08); 2008.

D'Atri E, Medaglia CM, Serbanati A, Ceipidor UB. A system to aid blind people in the mobility: a usability test and its results. In: Proceedings of the second international conference on systems (ICONS '07). Sainte-Luce, Martinique; 2007.

Domingo MC. A context-aware service architecture for the integration of body sensor networks and social networks through IP multimedia subsystem. IEEE Communications Magazine 2011;49(1):102–8.

Dunkels A, Vasseur JP. IP for smart objects. Internet protocol for smart objects (IPSO) alliance. White paper #1 July 2010. 〈http://ipso-alliance.org/〉 [original version September 2008].

EU FP7 Project CASAGRAS. CASAGRAS final report: RFID and the inclusive model for the internet of things; 2009.

Fazel-Rezai R. Recent advances in brain–computer interface systems. Rijeka, Croatia: InTech; 2011.

Fielding RT, Taylor RN. Principled design of the modern web architecture. ACM Transactions on Internet Technology (TOIT);2002;2(2):115–150.

Gershenfeld N, Cohen D. Internet 0: interdevice internetworking—end-to-end modulation for embedded networks. IEEE Circuits and Devices Magazine 2006;22(5):48–55.

Giner P, Cetina C, Fons J, Pelechano V. Developing mobile workflow support for the internet of things. IEEE Pervasive Computing 2010;9(2):18–26.

Haller S, Karnouskos S, Schroth C. The internet of things in an enterprise context. In: Proceedings of the first future internet symposium (FIS 2008), LNCS 5468. Springer Verlag; 2009.

Hengeveld B, Hummels C, Overbeeke K. Tangibles for toddlers learning language. In: Proceedings of the tangible and embedded interaction (TEI'09); 2009.

Hsu H-H, Lee Ch-N, Chen Y-F. An RFID-based reminder system for smart home. In: Proceedings of the IEEE international conference on advanced information networking and applications (AINA); March 2011.

ITU Internet Reports. The internet of things. Executive summary; November 2005. Available at: 〈http://www.itu.int/publ/S-POL-IR.IT-2005/e〉.

Jara AJ, Zamora MA, Skarmeta AFG.. An architecture based on internet of things to support mobility and security in medical environments. In: Proceedings of the seventh IEEE consumer communications and networking conference (CCNC 2010); January 2010.

Kranz M, Roalter L, Michahelles F. Things that twitter: social networks and the internet of things. In: Proceedings of the eighth international conference on pervasive computing (pervasive 2010), what can the internet of things do for the citizen (CIoT) workshop; May 2010.

Krishna S, Balasubramanian V, Krishnan NC, Hedgpeth T, Juillard C, Panchanathan S. A wearable wireless RFID system for accessible shopping environments. In: Proceedings of the third international conference on body area networks (BodyNets08). Tempe, USA; March 2008.

Kulyukin V, Kutiyanawala A. Accessible shopping systems for blind and visually impaired individuals: design requirements and the state of the art. The Open Rehabilitation Journal 2010;3:158–68.

Lanigan PE, Paulos AM, Williams AW, Rossi D, Narasimhan P. Trinetra: assistive technologies for grocery shopping for the blind. In: Proceedings of the IEEE-BAIS symposium on research in assistive technologies. Dayton, USA; April 2007.

Leal B, Atzori L. Objects communication behavior on multihomed hybrid ad hoc networks. In: Proceedings of the 20th Tyrrhenian workshop on digital communications: the internet of thing. Pula, Sardinia: Springer Verlag; September 2009.

López-de-Ipiña D, Lorido T, López U. Indoor navigation and product recognition for blind people assisted shopping. In: Proceedings of III international workshop of ambient assisted living (IWAAL). Málaga, Spain; June 2011.

Martin W, Dancer K, Rock K, Zeleny C, Yelamarthi K. The smart cane: an electrical engineering design project. In: Proceedings of ASEE north central section conference. Michigan, USA; 2009.

Millán J del R, Rupp R, Mueller-Putz G, Murray-Smith R, Giugliemma C, Tangermann M, et al. Combining brain–computer interfaces and assistive technologies: state-of-the-art and challenges. Frontiers in Neuroscience 2010;4:1–15.

Nano Retina. 〈http://www.nano-retina.com/〉.

Narasimhan P. Assistive embedded technologies. Computer 2006;39(7):85–7.
Nicholson J, Kulyukin V, Coster D. ShopTalk: independent blind shopping through verbal route directions and barcode scans. The Open Rehabilitation Journal 2009;2:11–23.
Organisation for Economic Co-operation and Development. Sickness, disability and work: breaking the barriers. A synthesis of findings across OECD countries. Paris: 2010.
Parton B, Hancock R. Interactive storybooks for deaf children. Journal of Technology Integration in the Classroom 2011;3:1.
Parton B, Hancock R, Crain-Dorough M, Oescher J. Interactive media to support language acquisition for deaf students. Journal on School Educational Technology 2009;5(1):17–24.
Parton B, Hancock R, Mihir F. Physical world hyperlinking: can computer-based instruction in a K-6 educational setting be easily accessed through tangible tagged objects? Journal of Interactive Learning Research 2010;21(1): 95–110.
Parton BS, Hancock R, duBusdeValempr AD. Tangible manipulatives and digital content: the transparent link that benefits young deaf children. In: Proceedings of the international conference on interaction design and children (IDC '10); 2010.
Pascual J, Sanjuán O, Cueva JM, Pelayo BC, Álvarez M, González A. Modeling architecture for collaborative virtual objects based on services. Journal of Network and Computer Applications 2011;34(5):1634–47.
Ren H, Meng MQH, Chen X. Wireless assistive sensor networks for the deaf. In: Proceedings of the international conference on intelligent robots and systems; October 2006.
Richard E, Billaudeau V, Richard P, Gaudin G. Augmented reality for rehabilitation of cognitive disabled children: a preliminary study. In: Proceedings of virtual rehabilitation; September 2007.
Saaid MF, Ismail I, Noor MZH. Radio frequency identification walking stick (RFIWS): a device for the blind. In: Proceedings of the fifth international colloquium on signal processing and its applications (CSPA'09); March 2009.
Sarji DK. HandTalk: assistive technology for the deaf. Computer 2008;41(7):84–6.
Satoh H, Kawabata T, Sankai Y. Bathing care assistance with robot suit HAL. In: Proceedings of the IEEE international conference on robotics and biomimetics (ROBIO); December 2009.
Schwiebert L, Gupta SKS, Weinmann J. Research challenges in wireless networks of biomedical sensors. In: Proceedings of MobiCom'01. Rome, Italy; 2001.
Shelby Z. Embedded web services. IEEE Wireless Communications 2010;17(6): 52–7.
Shelby Z, Bormann C. 6LoWPAN: the wireless embedded internet.Chichester, UK: John Wiley and Sons, Ltd.; 2009.
Shelby Z, Hartke K, Bormann C, Frank B. Constrained application protocol (CoAP). draft-ietf-core-coap-07; July 2011 [work in progress].
Shiizu Y, Hirahara Y, Yanashima K, Magatani K. The development of a white cane which navigates the visually impaired. In: Proceedings of the 29th annual international conference of the IEEE engineering in medicine and biology society (EMBS'07). Lyon, France; 2007.
Stefanov DH, Bien Z, Bang W-Ch. The smart house for older persons and persons with physical disabilities: structure, technology arrangements, and perspectives. IEEE Transactions on Neural Systems and Rehabilitation Engineering 2004;12(2):228–50.
Sun Ju J, Shin Y, Yi Kim E. Intelligent wheelchair (IW) interface using face and mouth recognition. In: Proceedings of the 13th international conference on intelligent user interfaces; 2009.
Tan L, Wang N. Future internet: the internet of things. In: Proceedings of third international conference on advanced computer theory and engineering (ICACTE'10). Chengdu, China; August 2010.
Tan W, Loeb GE. Feasibility of prosthetic posture sensing via injectable electronic modules. IEEE Transactions on Neural Systems and Rehabilitation Engineering 2007;15(2):295–309.
Velliste M, Perel S, Spalding MC, Whitford AS, Schwartz AB. Cortical control of a prosthetic arm for self-feeding. Nature 2008;453:1098–101.
Welbourne E, Battle L, Cole G, Gould K, Rector K, Raymer S, et al. Building the internet of things using RFID: the RFID ecosystem experience. IEEE Internet Computing 2009;13(3):48–55.
Wieland M, Kaczmarczyk P, Nicklas D. Context integration for smart workflows. In: Proceedings of the sixth annual IEEE international conference on pervasive computing and communications (PerCom 2008); March 2008.
Williamson R, Andrews BJ. Sensor systems for lower limb functional electrical stimulation (FES) control. Medical Engineering and Physics 2000;22:313–25.
Winlock T, Christiansen E, Belongie S. Toward real-time grocery detection for the visually impaired. In: Proceedings of the computer vision applications for the visually impaired workshop (CVAVI). San Francisco, USA; 2010.
World Health Organization (WHO). World report on disability; June 2011.
Yang Ch-H, Chien J-H, Wang B-Y, Chen P-H, Lee D-S. A flexible surface wetness sensor using a RFID technique. Biomedical Microdevices 2008;10(1):47–54.
Ye JH, Ryu SB, Kim KH, Goo YS. Retinal ganglion cell (RGC) responses to different voltage stimulation parameters in rd1 mouse retina. In: Proceedings of the 2010 annual international conference of the IEEE engineering in medicine and biology society (EMBC). Buenos Aires, Argentina; 2010.
Yelamarthi K, Haas D, Nielsen D, Mothersell S. RFID and GPS integrated navigation system for the visually impaired. In: Proceedings of IEEE international midwest symposium on circuits and systems; August 2010.
Zhang J, Lip CW, Ong SK, Nee A. A multiple sensor-based shoe-mounted user interface designed for navigation systems for the visually impaired. In: Proceedings of the fifth annual ICST wireless internet conference (WICON). Singapore; 2010.
Zorzi M, Gluhak A, Lange S, Bassi A. From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view. IEEE Wireless Communications 2010;17(6):44–51.

Why Countries Need National Strategies for the Internet of Things

By Joshua New & Daniel Castro | December 16, 2015

The Internet of Things offers many opportunities to grow the economy and improve quality of life. Just as the public sector was instrumental in enabling the development and deployment of the Internet, it must play a similar role to ensure the success of the Internet of Things. Therefore, national governments should create comprehensive national strategies for the Internet of Things to ensure that the technology develops cohesively and rapidly, that consumers and businesses do not face barriers to adoption, and that both the private and public sector take full advantage of the coming wave of smart devices.

A national strategy for the Internet of Things, if designed and implemented correctly, would maximize the opportunity for the Internet of Things to deliver substantial social and economic benefits.

Traditionally, most Internet users have been people: individuals sending email, reading the news, shopping online, and the like. But in the near future, most users will be machines: a vast array of ordinary devices that are equipped with sensors and networking capabilities so they can collect and share data with people and other devices. In fact, we are already well on our way toward building the Internet of Things (IoT). As the cost of deploying smart devices declines, homes, factories, farms, office buildings, and even cities are generating vast quantities of data that can be collected, analyzed, and acted upon. Data from these connected devices is creating tremendous opportunities to generate economic and social benefits, ranging from sensor-equipped bridges that can alert authorities if there is a risk of structural failure to waterways that can warn environmental regulators about spikes of fatally toxic algae.[1]

Smart public policies that proactively support innovation—or carefully avoid doing harm by restraining from the impulse to regulate or if needed, regulating with a light touch—have been integral to the success of major

technological developments such as the Internet, global positioning systems, and supercomputers.[2] Smart policies can foster the growth of the Internet of Things, too. Indeed, there is an even more compelling case for countries to craft comprehensive strategies for the Internet of Things, because, as this report details, there are a number of market failures that if left unaddressed can slow the technology's progress at the national level. Moreover, because many opportunities are strongly tied to areas of public-sector activity (such as health, environment, transportation, defense, and city management), comprehensive national strategies can ensure governments take full advantage of the Internet of Things to improve their own performance.

WHY THE INTERNET OF THINGS MATTERS

The Internet of Things will have a substantial impact on virtually all aspects of business and society. The number of new devices and services built for the Internet of Things has risen sharply in recent years, and connected devices are increasingly used to generate new insights into human health, improve public safety, conserve resources, boost productivity, and support more effective government.[3] Industry forecasters estimate that by 2020 there will be 26 to 50 billion connected devices in use worldwide.[4] While many smart devices provide immediate benefits in isolation, their benefits will multiply as their numbers increase and they generate more shareable data that leads to more actionable insights.

The Internet of Things is expected to contribute up to $11 trillion in value per year globally by 2025.[5] Companies can use the Internet of Things to become more efficient, for example by reducing downtime in factories as they constantly monitor machine performance to address issues before they become problematic, or as they use real-time data about customer demand to better manage supply chains.[6] And consumers can use the Internet of Things to save money, for example by using smart thermostats to reduce their energy bills or by using fitness trackers to earn lower health insurance premiums in exchange for demonstrably healthy behavior.[7]

For the global public sector specifically, the Internet of Things could generate $4.6 trillion by 2022 by increasing employee productivity, making military defense systems more effective, reducing costs, improving citizens' experience with public services, and increasing government revenue.[8] First responders can use the Internet of Things to save lives. For example, firefighters can use smart clothing to monitor environmental conditions and more safely respond to emergencies.[9] Cities can use the Internet of Things to operate more intelligently and better serve residents, such as by monitoring flows in water and sewage treatment plants in real time to reduce power consumption and costs; by installing parking sensors to help

people with disabilities quickly find accessible parking spaces; or by tracking snowplows in real time to better respond to residents' snow removal requests and identify where communities are being underserved.[10]

Ultimately, the Internet of Things is a platform for innovation that has the potential to be as disruptive and beneficial as the Internet itself has been. While industry forecasters and technologists can imagine its potential applications and estimate its impact, there is simply no way to predict all of or even most of the most of the opportunities that the Internet of Things will create. But, from the many connected devices and services that have already begun to reshape factories, hospitals, cities, and homes, there is no doubt that the Internet of Things will be one of the defining technologies of the first half of the twenty-first century.

WHY DO NATIONS NEED A NATIONAL INTERNET OF THINGS STRATEGY?

While the private sector can successfully develop many valuable technologies on its own, particularly those technologies with few network effects, the Internet of Things is different. To be sure, the private sector will be the primary driver of the Internet of Things as its potential benefits create enormous incentives to invest and deploy the technology. However, the Internet of Things is subject to an array of market failures that could limit these incentives and thus slow progress toward a fully connected world. Additionally, if poorly designed, government regulations can make deploying IoT technologies more expensive and less valuable. Furthermore, governments can help bridge the divide between those communities and individuals who are able to fully benefit from the Internet of Things and those who cannot based on market forces alone. Because of these three factors—market failures, the need for an innovation-friendly regulatory environment, and the need to promote equity—governments should develop comprehensive national strategies that remove obstacles and support development and widespread adoption of the technology.

MARKET FAILURES

If left solely to market forces, the development of the Internet of Things will fail to reach its full potential. These market failures include:

Externalities, Including Network Externalities

Many of the social and economic benefits from large-scale deployment of the technology accrue not to those buying or selling IoT products and services, but to competitors—through the expansion of network benefits—and to non-users, if the application generates an external benefit. One of these external benefits comes from the use of the data. An application that

can analyze billions of data points is more valuable to society, or to an individual company, than one that can tap only millions of data points. This phenomenon occurs for many networked technologies, since the value of a network rises as the number of users grows.[11]

Another externality is the generation of social benefits in areas such as health and energy. For example, a smart thermostat may save consumers money, but it can also reduce overall energy demand.[12] If certain consumers do not find the cost savings that smart thermostats can generate sufficient to warrant buying them, then the nation as a whole will suffer from increased energy prices and pollution. Likewise, when consumers use IoT applications to improve their health, some of the benefits go to society in the form of lower health-care costs. Because the consumer benefit is smaller than the social benefit, there will be underinvestment in IoT applications.

There are also externalities from increased scale. For many connected technologies, a greater number of users will bring down prices due to economies of scale in production, but individual buyers will receive only a tiny portion of this benefit.

"Chicken-and-Egg" Dynamics

The success of some IoT applications depends on the success of other technologies and vice versa. For example, some successful IoT application rollouts will depend on widespread adoption of smart phones and broadband Internet service. At the same time, more use of the Internet of Things will spur more broadband and smart phone adoption. Similarly, some vehicle applications that rely on the Internet of Things would have more value if all infrastructures were IoT-enabled—from traffic lights to toll booths to railroad crossings. Another example concerns near field communication (NFC) technology.[13] NFC technology allows electronic devices to share data with each other when they are in close proximity and can power applications such as from smartphone "wallets." Though NFC technology has existed for some time, consumers have had little reason to demand it in new smartphones because they have had scant opportunities to use it; and in the absence of demand from a large base of customers, stores have had little reason to invest in NFC payment systems.[14] However, countries like Japan and South Korea have successfully induced a wide variety of market players to adopt the technology, from retailers to banks to public transit authorities.[15] As a result, the Asia Pacific region has captured the overwhelming majority of value of the global NFC payment market, which is expected to reach $21.8 billion by 2020.[16]

While the market may eventually be able to establish effective interdependent systems, it would take longer and happen much more

incrementally than it would with government support to resolve chicken-and-egg dilemmas and encourage mutual adoption of these technologies until market forces can take over and drive full deployment.

Risk and Uncertainty

Because the Internet of Things represents an emerging set of technologies, many potential users, including companies and local governments, will disregard the benefits it promises and delay adoption until the technology is proven. Economists refer to this challenge as excess inertia or, more commonly, "the penguin effect"—in a group of hungry penguins, no individual penguin is willing to be the first to enter the water to search for food due to the risk of encountering a predator. Yet if no penguin is willing to test the waters, then the whole group risks starvation.[17]

Governments have much to gain from adopting connected technologies, but when they do so, they are not the only ones that benefit; they help the entire IoT ecosystem. As early and lead adopters, governments can help spur development and growth of the entire ecosystem by helping to reduce risk and by encouraging others to invest in the technology. However, without a national strategy to drive this adoption, government agencies will be less likely to consider the external benefits when weighing whether to integrate the Internet of Things into their operations.

Competitiveness Externalities

The Internet of Things offers a valuable opportunity for countries to gain a competitive advantage in the global marketplace. Those that are home to companies well-positioned to produce billions of new connected devices, develop software to run them, and apply analytics to generate value from the data they generate will have a competitive advantage over other countries. Similarly, given the efficiency and productivity gains the technology can offer the private sector, countries that readily adopt and implement the Internet of Things will gain a competitive edge over those that do not.

While business actions can improve an individual firm's competitiveness, everyone, not just the individual firm, shares in the benefits of a national economy that is more competitive overall.[18] But the drawbacks of an uncompetitive economy work the same way: if a country is not well-positioned to develop or adopt the Internet of Things, its national economy will be less competitive overall and individual businesses can be at a relative disadvantage in the global marketplace. For example, an importer that implements connected technologies to improve the efficiency of its international supply chains and reduce overhead costs will increase the overall competitiveness of domestic companies that can purchase

imported goods at resulting lower prices.[19] Conversely, companies in a country slower to adopt this technology, through no fault of their own, will find themselves at a competitive disadvantage as a result of comparatively sluggish supply chains.

Interoperability

The private sector can and should lead the development and adoption of standards for the Internet of Things. However, standards coordination is important in public-sector applications. In the past, the lack of national coordination has led to incompatible systems and lagging adoption. During the last two decades, for example, some U.S. states have implemented radio-frequency identification systems to allow drivers to easily pay highway and bridge tolls, but they have deployed these systems independently of one another, leading to a patchwork of incompatible systems from state to state.[20] Earlier federal efforts to support interoperability and widespread deployment would have made these toll payment systems more useful to drivers.

While local governments should be encouraged to experiment with the Internet of Things, national governments have an important coordinating role to play in developing large-scale deployments of sensor networks and smart infrastructure that spans multiple jurisdictions. For example, in June 2014, the UK government's Technology Strategy Board provided $12.1 million to convene an industry working group to develop an open standard for the Internet of Things called HyperCat, designed to reduce the need for additional software to facilitate data sharing between new connected devices.[21] In January 2015, the group, with support from the Technology Strategy Board, launched an initiative called HyperCatCity to encourage the adoption of the HyperCat standard by technology firms working with public-sector agencies to support the interoperability of different smart city technologies as they are developed for multiple cities.[22]

Additionally, certain countries may mandate the use of particular standards within their borders in an effort to support domestic business interests. However, nation-specific standards limit the ability of international companies to enter domestic markets and actually reduce domestic firms' ability to compete internationally.[23]

Public Goods

Certain aspects of the Internet of Things require public goods that the private sector cannot or will not adequately provide. National strategies should ensure the public sector provides these necessary public goods, which include:

Human Capital

The value of the Internet of Things, and thus the willingness of the public and private sector to develop and implement the technology, hinges upon the data it generates. But no country will be able to fully capture this value without a workforce equipped with the necessary skills. By 2018, the United States will face a shortage of up to 190,000 workers well-educated in data science and 1.5 million managers and analysts able to use data to make better decisions.[24] Similarly, a survey of 497 businesses in the China, France, Germany, India, the United Kingdom, and the United States revealed that this shortage of skilled data workers is a universal concern, with only one-third of companies reporting they have the human capital necessary to effectively use new data.[25] The public sector will likely feel the impact of this skills shortage more severely than the private sector, because businesses will be able to offer more competitive salaries as data skills become even more in demand, while governments will struggle to attract comparable talent.

While businesses can provide some supplementary training for employees, only government efforts to encourage the cultivation of data science skills in high school and higher education can meaningfully reduce the human capital shortages that stand to limit the benefits of the Internet of Things.

Radio Spectrum

The Internet of Things will consist of billions of connected devices communicating with one another, and this influx of new connected devices will create demands for spectrum frequency space that many national spectrum licensing regimes will likely be unable to support. If too many transmitting devices compete for spectrum, they will be unable to share data with each other or operate effectively.

Many applications in the Internet of Things, such as smart home devices and networked assembly lines, can operate on local Wi-Fi networks and thus not take up much radio frequency space—a practice known as Wi-Fi offloading.[26] However, many applications of the Internet of Things will have unique technical requirements that Wi-Fi is not well-suited to support. For example, a sensor network dispersed through miles of farmland will need to utilize spectrum bands that can transmit data over long distances, but it will likely not need to transmit a high volume of data. As more specialized applications of the Internet of Things emerge and more devices rely on spectrum, governments will likely need to make available greater amounts of licensed and unlicensed spectrum. Some countries have already begun to explore how they can anticipate the spectrum needs of the Internet of Things. For example, in July 2014, the French telecommunication regulator solicited public comments about how it could be forward-looking in its

provision of unlicensed spectrum for connected devices.[27] And in September 2015, the Ministry of Economic Affairs in the Netherlands published a report examining the impact of the Internet of Things on radio spectrum, which recommended that the government closely monitor how new connected devices could contribute to bottlenecks in both licensed and unlicensed spectrum and investigate how it could provide additional spectrum to support critical IoT applications.[28]

Research and Development Funding

Substantial government investment in research and development (R&D) played a critical role in developing many vital technologies, including smartphones, search engines, genomic sequencing, and, of course, the Internet.[29] Thus, the Internet of Things, which offers equal or potentially greater value than these examples, should be a high priority for government R&D spending. Countries with robust technology sectors already leading the development of the Internet of Things may not feel the need to invest in R&D as urgently.[30] However, countries in this position should recognize that public and private R&D investments are complementary, rather than interchangeable, as public-sector R&D can advance research in areas that benefit all market players, such as scientific measurement.[31] In fact, government R&D spurs an increase in private-sector R&D spending, which can help accelerate the growth of the Internet of Things and give countries with already robust private sectors a competitive edge.[32]

INNOVATION-FRIENDLY REGULATION

Excessive or poorly-designed regulations can significantly slow the growth of the Internet of Things. Yet some policymakers have suggested that they want to develop new rules and regulations specifically for the Internet of Things, particularly as it relates to privacy.[33] For example, the U.S. Federal Trade Commission has expressed support for requiring the practice of data minimization for data generated by the Internet of Things—limiting the collection and retention of data so it can only fulfill specific, predefined purposes.[34] Applying such rules to the Internet of Things would be damaging as there may be one primary reason to collect data, but innumerable other ways to use the same data beneficially beyond its initial purpose. And, with so many new opportunities to collect data from billions of new connected devices, the value of the data at stake is proportionately large. Furthermore, mandating data minimization practices can preclude opportunities for de-identification, which can protect sensitive information without unnecessarily sacrificing its value.[35]

Similarly, it would be damaging to apply existing notification and consent rules to devices that gather consumer data on the Internet to the Internet

of Things, because many connected devices will have limited, if any, user interfaces.[36] Outdated notification requirements will prove particularly frustrating given that the vast majority of applications on the Internet of Things pose no real threat to consumer welfare and most data collection would likely be routine and insignificant. Any costs incurred by adhering to these regulations would be passed on to consumers and ultimately serve to make consumers less likely to adopt connected devices.

Companies also face the prospect of multiple regulators creating a confusing and disjointed patchwork of regulations. Whereas a company making a device for a car previously may have worked with a single government agency, a company developing connected devices for cars today could very well be subject overlapping or inconsistent rules from a consumer protection regulator, a transportation safety regulator, and a spectrum regulator, among others. Not only should countries strive to reduce counterproductive regulations, they should also curtail enactment of multiple regulatory frameworks that serve as barriers to new products and services, and instead simplify the regulatory process for innovators.

Some nations also want to restrict how data can flow across borders. India requires gateways and application servers that support the Internet of Things to be located inside the country if they service Indian customers. The rationale is to protect national security, even though such localization requirements have no impact on security whatsoever.[37] Such requirements limit the ability of international device manufacturers and service providers to analyze data collected from the Internet of Things around the world, thereby reducing the technology's potential value.[38]

Creating restrictive rules for an emerging technology at such an early stage in its development without clear evidence of concrete consumer harms can have the unintended consequence of limiting innovation by unnecessarily hampering certain business models or raising costs. Moreover, the privacy fears associated with new technologies are often substantially inflated.[39]

A national strategy for the Internet of Things can forestall such problems by sending a clear message to legislators and regulators that this technology is important and that over-regulation or poorly-designed regulation would limit its growth. Moreover, a national strategy can encourage legislators and regulators to focus on regulations that would expand, rather than limit use of the Internet of Things. For example, regulations designed to free up energy consumption data from smart meters, which are traditionally locked down by utility companies, can empower consumers to reduce their energy use and spur the development of new analytics services.[40] And in the United States, the E-LABEL Act of 2014 allowed manufacturers of certain connected devices to provide regulatory labeling information in an

electronic format through device displays, rather than on physical labels.[41] This simple change reduces overhead costs for device manufacturers and provides consumers with a greater amount of useful information.[42]

EQUITY

The Internet of Things can be a valuable tool to help meet the needs of underserved populations, but without appropriate public policies such as ensuring that smart city technologies serve all cities and neighborhoods rather than just affluent ones, adoption will be uneven. Failure to do so will limit the value of such systems as a whole because of the network effects that widespread deployments generate. For example, smart city technology that police departments use to reduce crime would be substantially less effective if they could only analyze data from certain neighborhoods.

A more pressing concern for governments is that many people and communities live in "data poverty"—the result of a routine lack of inclusion in public and private data collection efforts.[43] As the world increasingly relies on data to improve services such as health care, education, and finance, the potential harm of being underrepresented or excluded in the data that drives this decision-making also increases.[44] The Internet of Things offers a valuable opportunity to close this divide. Low-cost sensor technologies and networked services empower underserved populations to more easily provide data that is useful for improving their quality of life. However, this can only happen if governments invest in and deploy these technologies equitably. If the public sector does not take this into account, the Internet of Things could exacerbate existing inequalities by providing the benefits of data-driven decision-making only to some, and placing already underserved communities at an even greater disadvantage.[45]

NATIONAL EFFORTS TO SUPPORT THE INTERNET OF THINGS

Many nations have already recognized that the Internet of Things should be a high priority for the government, and some have even gone as far as to develop strategies to support the technology. However, none have developed and implemented a sufficiently comprehensive Internet of Things strategy.

CHINA

In March 2010, the Chinese central government committed $117.2 million to boost national competitiveness by opening a national center devoted to Internet of Things R&D.[46] Since then, the government has launched several IoT initiatives. In 2011, China's Ministry of Industry and Information Technology issued a Five-Year Plan for the Development of the Internet of Things, outlining how the government intends to support the technology,

such as by setting standards and demonstrating real-world applications. This plan called for creating an Internet of Things "Special Fund" to support R&D with investments totaling $774 million for the period of 2011 to 2015.[47] In August 2013, China's State Council issued guidance to support smart city pilot programs, with a particular focus on smart utilities and transportation, and the Chinese Development Bank agreed to establish financing programs for smart city pilots.[48] Also in 2013, China established an inter-agency council to guide national policy on the Internet of Things and issued guidance to support the technology, including fostering industry development, workforce training, and R&D targets.[49]

GERMANY

The Internet of Things is a main focus of Germany's "Industry 4.0" plan to modernize its manufacturing sector.[50] Germany has devoted $221 million to support industry, academic, and government research and development efforts to advance "smart factory" technologies ranging from sensor-embedded systems to artificial intelligence platforms that can help operate Internet-connected machinery.[51]

INDIA

India's National Telecom M2M (Machine-to-Machine) Roadmap, published in May 2015, established a policy framework to support digitization efforts and grow the Internet of Things.[52] The roadmap outlines opportunities the Internet of Things can offer for a wide variety of public- and private-sector applications, and details ongoing and planned government efforts to facilitate growth and adoption.[53] These efforts include providing government-backed venture capital funding, creating incubators and test bed facilities to support the growth of the Internet of Things, carrying out smart grid pilot programs, and working with educational institutions to provide the workforce with data skills.[54] The roadmap also outlines the government's ambitious plan to develop 100 smart cities, which it will finance with a $7.4 billion investment over the next five years.[55] India's smart city plan also calls on state and municipal governments to match national funding for smart cities.[56]

However, several of the provisions in India's roadmap designed to grow the Internet of Things would do the exact opposite.[57] For example, the roadmap details plans to require import licenses for certain types of connected devices, which could allow the government to charge foreign device manufacturers high fees to access Indian markets or block them from Indian markets outright. This policy necessarily reduces the ability of Indian consumers and businesses to take advantage of the best and most cost-effective connected devices and services, limiting their willingness to invest in the Internet of Things.

JAPAN

In June 2013, Japan declared it would strive to make the country the "world's most advanced IT nation," and announced a series of measures to harness the Internet of Things to develop solutions in the areas of healthcare, disaster resilience, public safety, and infrastructure planning, as well as encourage sensor technology R&D.[58] And in July 2015, the Japanese government announced plans to establish a council of public- and private-sector organizations to support the development and implementation of specific Internet of Things technologies by the end of 2018, including information processing technologies that can analyze the large amounts of data from connected devices, and systems for safely disabling Internet-connected autonomous devices such as self-driving cars in the event of a safety or security risk.[59]

SINGAPORE

In May 2005, Singapore unveiled its Intelligent Nation 2015 10-year plan to support the growth of the information and communications technology industry. This plan focuses in part on supporting the development and deployment of sensor networks and developing the communication infrastructure necessary to support ubiquitous connectivity.[60] In November 2014, Singapore also launched its Smart Nation initiative to secure economic and social benefits through greater adoption and cohesive use of technology, particularly the Internet of Things.[61] Singapore has allocated $1.6 billion in for the Smart Nation initiative for 2015, and while not all of aspects of the initiative are related to the Internet of Things, the funding will focus prominently on large-scale deployments of smart city applications.[62] And in August 2015, a group of government agencies began work on guidance to define standards for the Internet of Things, such as sensor network standards and domain-specific standards, to support the Smart Nation initiative and private-sector deployment of the technology.[63]

SOUTH KOREA

South Korea has $5 billion in planned investments in the Internet of Things through 2020 to support industries ranging from wearables to smart cars.[64] In October 2014, the South Korean Ministry of Science, Information Communications Technology, and Future Planning released a roadmap for the Internet of Things to guide government actions to develop cybersecurity standards and best practices.[65] South Korea has also built the Songdo International Business District, the world's first purpose-built smart city, with the help of government funding.[66]

UNITED STATES

The White House in September 2015 launched its Smart Cities Initiative, which encapsulates the majority of the U.S. government's efforts to support the Internet of Things and outlines $160 million in new and ongoing R&D funding that covers more applications than just smart cities.[67] The Smart Cities Initiative includes support for a range of programs including the National Institute of Standards and Technology's Global City Teams Challenge, which encourages the development of smart city applications, Internet-connected vehicle pilots, and the establishment of Internet of Things research test beds.[68] The federal government's Networking and Information Technology Research and Development Program also released its Smart Cities and Connected Communities Framework—a short guide to coordinate federal agency investment and collaboration for smart city technology.[69] In October 2015, the White House released its Strategy for American Innovation, which highlights the value of the Internet of Things for applications ranging from environmental monitoring to supply chain management.[70] And in December 2015, the Department of Transportation launched the Smart City Challenge, which will award $40 million in March 2016 to a mid-sized city to implement connected technologies to reduce congestion, improve transportation safety, protect the environment, and support economic growth.[71]

Country	Funding
China	$774 million over five years
India	$7.4 billion for smart cities
Germany	$221 million for smart factories
South Korea	$5 billion over five years
United States	$200 million

Table 1: Ongoing and recently launched government funding for the Internet of Things for select countries.

POLICIES FOR NATIONAL STRATEGIES

Every nation is different, so there is no "one-size-fits-all" approach to developing a national strategy. Yet, while specific policy considerations will vary from country to country, all national strategies will have to include a broad array of policies that focus in particular on funding, convening and planning, agency action, regulatory action, and trade. These include:

Funding

- Funding local government efforts to implement connected technologies and services;
- Funding large-scale national pilot projects for smart cities that focus on integrating multiple smart city applications with scalable and replicable solutions;[72]
- Establishing national challenges with prizes to spur the development of IoT applications with high social or economic impact;
- Subsidizing key connected devices for low-income populations;[73]
- Funding R&D for key underlying technological challenges relevant to the Internet of Things, such as improving cyber security and reducing power consumption; and
- Establishing government-backed venture capital funding for promising connected technologies that could benefit public sector operations.

Convening and Planning

- Encouraging robust public-private partnerships for ambitious civic technology projects;
- Facilitating local government smart city deployments, such as by providing best practices and financing guides and freely accessible software tools;
- Coordinating public sector deployments of sensor networks, particularly for applications spanning multiple jurisdictions; and
- Encouraging the development of industry-led voluntary standards and best practices around issues like privacy and security.

Agency Action

- Requiring relevant government agencies to develop and follow Internet of Things action plans focused on improving agency mission delivery with connected technologies;
- Revising procurement and grant policies to encourage deployment of connected devices;
- Making “smart” the default for government operations, such as by requiring the use of connected technologies for customs inspections, integrating smart technologies into government-subsidized housing and agency buildings; and embedding sensor networks into infrastructure as part of modernization efforts;[74] and
- Supporting data science skills in high school and higher education.

Regulatory Action

- Allocating additional licensed and unlicensed spectrum for connected devices;
- Ensuring that any consumer protection rules are narrow and targeted;[75]
- Minimizing the regulatory cost of data collection;[76]
- Fast-tracking regulatory review and approval for smart devices in regulated industries, such as connected medical devices;[77]
- Enacting regulations to increase the potential for data-driven innovation from connected devices, such as by giving public utility consumers access to their smart meter data; and
- Revising accessibility requirements for people with disabilities based on the opportunities created by connected technologies, such as dynamically adjusting the amount of accessible parking spaces based on sensor data indicating demand.

Trade Policy

- Ensuring that companies can freely exchange data across local and national borders;
- Promoting access to the best and most cost effective connected devices and services, such as by eliminating policies that restrict the ability of international device manufacturers to enter domestic markets; and
- Supporting voluntary, industry-led standards and fighting against nation-specific standards.

CONCLUSION

A national strategy for the Internet of Things, if designed and implemented correctly, would maximize the opportunity for the Internet of Things to deliver substantial social and economic benefits. No country will successfully capture these benefits by leaving development of the Internet of Things solely up to the market, just as no government actions could capture all of the potential benefits without a robust private sector that can innovate unencumbered by overly restrictive regulations. As countries increasingly recognize the potential of the Internet of Things, they should develop comprehensive national strategies that proactively promote development and adoption of the technology while limiting regulatory barriers that restrict its growth.

REFERENCES

1. Daniel Castro and Joshua New, "10 Policy Principles for Unlocking the Potential of the Internet of Things," Center for Data Innovation, December 4, 2015, http://www2.datainnovation.org/2014-iot-policy-principles.pdf; Joshua New, "The Internet of Things Could Stop Our Waterways from Dying," Center for Data Innovation," June 8, 2015, http://www.datainnovation.org/2015/06/the-internet-of-things-could-stop-our-waterways-from-dying/; Daniel Castro and Jordan Misra, "The Internet of Things," Center for Data innovation, November 2013, http://www2.datainnovation.org/2013-internet-of-things.pdf.

2. Peter Singer, "Federally Supported Innovations: 22 Examples of Major Technology Advances That Stem From Federal Research Support," Information Technology and Innovation Foundation, February 2014, http://www2.itif.org/2014-federally-supported-innovations.pdf.

3. Daniel Castro and Jordan Misra, "The Internet of Things," Center for Data innovation, November 2013, http://www2.datainnovation.org/2013-internet-of-things.pdf.

4. "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020," Gartner, December 12, 2013, http://www.gartner.com/newsroom/id/2636073, and "Broadband by the Numbers," National Cable & Telecommunications Association, https://www.ncta.com/broadband-by-the-numbers.

5. James Manyika et al., "Unlocking the Potential of the Internet of Things," McKinsey Global Institute, June 2015, http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.

6. Daniel Castro, "Data is the Key to the Factory of the Future," Center for Data Innovation, October 2, 2014, http://www.datainnovation.org/2014/10/data-is-the-key-to-the-factory-of-the-future/; Daniel Castro and Joshua New, "10 Policy Principles for Unlocking the Potential of the Internet of Things," Center for Data Innovation, December 4, 2015, http://www2.datainnovation.org/2014-iot-policy-principles.pdf; Joshua New, "5 Q's for Steve Hershberger, CEO of SteadyServ Technologies," Center for Data Innovation, April 13, 2015, http://www.datainnovation.org/2015/04/5-qs-for-steve-hershberger-ceo-of-steadyserv-technologies/.

7. "Energy Savings from the Nest Learning Thermostat: Energy Bill Analysis Results," Nest Labs, February 2015, https://nest.com/downloads/press/documents/energy-savings-white-paper.pdf, and Parmy Olson, "Apple's iPhone Just Stepped Closer to Shaping Your Health Care Costs," Forbes, October 1, 2015,

http://www.forbes.com/sites/parmyolson/2014/10/01/apple-iphone-healthkit-humana-insurance-partnership/.

8. Joseph Bradley et al., "Internet of Everything: A $4.6 Trillion Public-Sector Opportunity," Cisco, 2013, http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf.

9. Casey Grant et al., "Research Roadmap for Smart Fire Fighting," National Institute of Standards and Technology, May 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1191.pdf.

10. Parul Bhandari, "Governments Worldwide Embracing IoT," November 24, 2015, Microsoft, http://www.microsoft.com/en-us/government/blogs/governments-worldwide-embracing-iot/default.aspx#fbid=Y1jCXcaphoj; Lambros Lambrinos and Aristotelis Dosis, "Applying Mobile and Internet of Things Technologies in Managing Parking Spaces for People with Disabilities," UbiComp, September 8, 2013, http://www.ubicomp.org/ubicomp2013/adjunct/adjunct/p219.pdf; and Terrell McSweeny, "Keynote Remarks of Commissioner Terrell McSweeny," Federal Trade Commission, September 10, 2015, https://www.ftc.gov/system/files/documents/public_statements/800981/150909googletechroundtable.pdf.

11. "Network Effect," Investopedia, http://www.investopedia.com/terms/n/network-effect.asp.

12. "Energy Savings from the Nest Learning Thermostat: Energy Bill Analysis Results," Nest Labs, February 2015, https://nest.com/downloads/press/documents/energy-savings-white-paper.pdf

13. Robert Atkinson and Stephen Ezell, Innovation Economics: The Race for Global Advantage, (New Haven: Yale University Press, 2012).

14. Ibid.

15. Ibid.

16. "Near Field Communication Market by Operating Mode, Indusry, and Geography – Global Forecast to 2020," Markets and Markets, November 2015, http://www.marketsandmarkets.com/Market-Reports/near-field-communication-nfc-market-520.html, and "Increased Adoption of Contactless Payments in Japan, South Korea," The Paypers, April 17, 2014, http://www.thepaypers.com/mobile-payments/increased-adoption-of-contactless-payments-in-japan-south-korea/754854-16.

17. Tim Weitzel, Economics of Standards in Information Networks, (Physica-Verlag Heidelberg, 2004), https://books.google.com/books?id=Ae37CAAAQBAJ&printsec=frontcover#v=onepage&q&f=false.

18. The true definition of competitiveness is the ability of a region to export more in value added terms than it imports. This calculation includes accounting for "terms of trade" to reflect all government "discounts," including an artificially low currency, suppressed wages in export sectors, artificially low taxes on traded sector firms and direct subsidies to exports. It also controls for both tariff and non-tariff barriers to imports. Robert Atkinson, "Competitiveness, Innovation, and Productivity: Clearing up the Confusion," Information Technology and Innovation Foundation, August 2013, https://itif.org/publications/2013/08/19/competitiveness-innovation-and-productivity-clearing-confusion.

19. Daniel Castro and Joshua New, "Accelerating Data Innovation: A Legislative Agenda for Congress," Center for Data Innovation, May 11, 2015, http://www2.datainnovation.org/2015-data-innovation-agenda.pdf.

20. Eric Jaffe, "You May Never Need to Pay Cash at a Toolbooth Again," CityLab, August 12, 2013, http://www.citylab.com/tech/2013/08/you-may-never-need-pay-cash-tollbooth-again/6497/.

21. Ryan Daws, "Britain wants HyperCat to Reign the Internet of Things," TelecomsTech, August 21, 2014, http://www.telecomstechnews.com/news/2014/aug/21/britain-wants-hypercat-reign-internet-things/.

22. Daniel Robinson, "HyperCatCity Initiative Looks to Kickstart Smart Cities by Opening Up Data," V3, January 27, 2015, http://www.v3.co.uk/v3-uk/news/2392084/hypercatcity-initiative-looks-to-kickstart-smart-cities-by-opening-up-data.

23. Stephen Ezell and Robert Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards," Information Technology and Innovation Foundation, December 2014, http://www2.itif.org/2014-galapagos-chinese-ict.pdf.

24. James Manyika et al., "Big Data: The Next Frontier for Innovation, Competition, and Productivity," McKinsey Global Institute, May 2011, http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

25. "Data Science Revealed: A Data-Driven Glimpse into the Burgeoning New Field," EMC, 2011, http://www.emc.com/collateral/about/news/emc-data-science-study-wp.pdf.

26. Jack Schofield, “Most Mobile Data Will Soon Be Offloaded to Wi-Fi Networks, Says Juniper Research,” ZDNet, June 12, 2013, http://www.zdnet.com/article/most-mobile-data-will-soon-be-offloaded-to-wi-fi-networks-says-juniper-research/.

27. “ARCEP Launches a Public Consultation on the Use of Open Spectrum, ARCEP, July 25, 2014, http://www.arcep.fr/index.php?id=8571&tx_gsactualite_pi1%5Buid%5D=1683&L=1&cHash=c9f8d378812b7725159f52eed4314e35.

28. Stratix, “Internet of Things in the Netherlands,” Rjksoverheid, September 2015, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/10/08/internet-of-things-in-the-netherlands/rapport-internet-of-things-in-the-netherlands.PDF.

29. Peter Singer, “Federally Supported Innovations: 22 Examples of Major Technology Advances That Stem From Federal Research Support,” Information Technology and Innovation Foundation, February 2014, http://www2.itif.org/2014-federally-supported-innovations.pdf, and Bernhard Warner, “Why Private Companies Won’t Make Up for Cuts in government Science Funding,” Bloomberg, March 5, 2013, http://www.bloomberg.com/bw/articles/2013-03-05/why-private-companies-wont-make-up-for-cuts-in-government-science-funding.

30. Kevin Ashton, “America Last?” Politico, June 2015, http://www.politico.com/agenda/story/2015/06/kevin-ashton-internet-of-things-in-the-us-000102.

31. Brad Plumer, “The Coming R&D Crash,” Washington Post, February 26, 2013, https://www.washingtonpost.com/news/wonk/wp/2013/02/26/the-coming-rd-crash/, and “Metrology and Standards,” The Innovation Policy Platform, 2013, https://www.innovationpolicyplatform.org/content/metrology-and-standards.

32. Justin Hicks and Robert Atkinson, “Eroding Our Foundation: Sequestration, R&D, Innovation, and U.S. Economic Growth,” Information Technology and Innovation Foundation, September 2012, http://www2.itif.org/2012-eroding-foundation.pdf.

33. Julie Brill, “Keynote Address for EuroForum European Data Protection Days,” Federal Trade Commission, May 4, 2015, https://www.ftc.gov/system/files/documents/public_statements/640741/2015-05-04_euroforum_iot_brill_final.pdf.

34. "Internet of Things: Privacy & Security in a Connected World," Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

35. Ann Cavoukian and Daniel Castro, "Big Data and Innovation, Setting the Record Straight: De-identification Does Work," Information Technology and Innovation Foundation, June 16, 2014, http://www2.itif.org/2014-big-data-deidentification.pdf.

36. For example, California's Online Privacy Protection Act of 2003 requires companies that collect personal data from users of their website to clearly display their privacy policies, and the Federal Trade Commission's (FTC) Behavioral Advertising Principles suggests website operators notify users about their data collection practices. "California Online Privacy protection Act of 2003," Cooley Godward LLP, June 2004, https://cooley.com/files/ALERT-Cal_OPPA.pdf, and Leuan Jolly, "Data Protection in United States: Overview," Practical Law, July 1, 2015, http://us.practicallaw.com/6-502-0467#a904003.

37. "National Telecom M2M Roadmap," Ministry of Communications & Information Technology, May 2015, http://www.dot.gov.in/sites/default/files/u10/National%20Telecom%20M2M%20Roadmap.pdf, and Daniel Castro, "The False Promise of Data Nationalism," Information Technology and Innovation Foundation, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

38. Daniel Castro, "The False Promise of Data Nationalism," Information Technology and Innovation Foundation, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

39. Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies," Information Technology and Innovation Foundation, September 2015, http://www2.itif.org/2015-privacy-panic.pdf.

40. Daniel Castro and Joshua New, "Accelerating Data Innovation: A Legislative Agenda for Congress," Center for Data Innovation, May 11, 2015, http://www2.datainnovation.org/2015-data-innovation-agenda.pdf.

41. E-LABEL Act of 2014, S. 2583, 113th Congress. (2014).

42. Alan McQuinn, "Proposed E-Labeling Act a Homerun for Internet of Things," Industry Week, July 25, 2014, http://www.industryweek.com/technology/proposed-e-labeling-act-homerun-internet-things.

43. Daniel Castro, “The Rise of Data Poverty in America,” Center for Data Innovation, September 10, 2014, http://www2.datainnovation.org/2014-data-poverty.pdf.

44. Ibid.

45. Ibid.

46. “Shangai Launches First Internet of Things Center,” China Daily, March 2, 2010, http://www.chinadaily.com.cn/china/2010-03/02/content_9527480.htm.

47. “物联网十二五规划或9月出台 产业规模或超5千亿,” Ministry of Finance of the People’s Republic of China, August 24, 2011, http://www.mof.gov.cn/zhengwuxinxi/caijingshidian/jjckb/201108/t20110824_588476.html.

48. Ken Yaron et al., “Comparative Study of Smart Cities in Europe and China,” EU-China Policy Dialogues Support Facility II, March 2014, http://euchina-ict.eu/wp-content/uploads/2015/01/Smart_City_report_draft-White-Paper-_-March-2014.pdf.

49. “How China is Scaling the Internet of Things,” The GSM Association, July 2015, http://www.gsma.com/newsroom/wp-content/uploads/16531-China-IoT-Report-LR.pdf.

50. “Industrie 4.0,” Germany Trade & Invest, http://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Brochures/Industries/industrie4.0-smart-manufacturing-for-the-future-en.pdf.

51. Ibid, and Sara Zaske, “Germany’s Vision for Industrie 4.0: The Revolution Will Be Digitised,” ZDNET, February 23, 2015, http://www.zdnet.com/article/germanys-vision-for-industrie-4-0-the-revolution-will-be-digitised/.

52. “National Telecom M2M Roadmap,” Ministry of Communications & Information Technology, May 2015, http://www.dot.gov.in/sites/default/files/u10/National%20Telecom%20M2M%20Roadmap.pdf, and Joshua New, “What India Gets Right, and Wrong, About the Internet of Things, Center for Data Innovation, June 16, 2015, http://www.datainnovation.org/2015/06/what-india-gets-right-and-wrong-about-the-internet-of-things/.

53. Ibid.

54. Ibid.

55. "Mission Statement & Guidelines," Ministry of Urban Development, June 2015, http://smartcities.gov.in/writereaddata/SmartCityGuidelines.pdf.

56. Ibid.

57. Joshua New, "What India Gets Right, and Wrong, About the Internet of Things, Center for Data Innovation, June 16, 2015, http://www.datainnovation.org/2015/06/what-india-gets-right-and-wrong-about-the-internet-of-things/.

58. "Declaration to Be the World's Most Advanced IT Nation," Kantei, June 14, 2013, http://japan.kantei.go.jp/policy/it/2013/0614_declaration.pdf.

59. "Japanese Government to Set Up Council for 'Internet of Things' Development," Daily Herald, July 18, 2015, http://www.dailyherald.com/article/20150718/business/150719510/.

60. "iN2015 Masterplan," Infocomm Development Authority of Singapore, https://www.ida.gov.sg/Tech-Scene-News/iN2015-Masterplan, and iN2015 Infocomm Infrastructure, Services and Technology Development Sub-Committee, "Totally Connected, Wired and Wireless," Infocomm Development Authority of Singapore, June 2006, https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/iN2015/Reports/09_Infocomm_Infrastructure_Services_and_Technology_Devt.pdf.

61. Rachel Au-Yong, "Vision of a Smart Nation is to Make Life Better: PM Lee," Straits Times, November 25, 2014, http://www.straitstimes.com/singapore/vision-of-a-smart-nation-is-to-make-life-better-pm-lee.

62. Faris Mokhtar, "Governments to Launch S$2.2b in ICT Tenders to Realise Smart Nation Vision," Channel NewsAsia, August 22, 2015, http://www.channelnewsasia.com/news/business/government-to-launch-s-2/1874506.html, and Eileen Yu, "Singapore Unveils Plan in Push to Become Smart Nation," ZDNet, June 17, 2014, http://www.zdnet.com/article/singapore-unveils-plan-in-push-to-become-smart-nation/.

63. Vivian Balakrishnan, "Speech by Dr. Vivian Balakrishnan at the Quality and Standards Conference 2015," Spring Singapore, August 12, 2015, http://www.spring.gov.sg/NewsEvents/PS/Pages/Speech-by-Dr-Vivian-Balakrishnan-at-the-Quality-and-Standards-Conference-2015-20150812.aspx, and "SPRING Singapore Supported Close to 600 Companies in Standards Adoption, and Service Excellence Projects," SPRING Singapore, August 12, 2015, http://www.spring.gov.sg/NewsEvents/PR/Pages/Internet-of-Things-(IoT)-

Standards-Outline-to-Support-Smart-Nation-Initiative-Unveiled-20150812.aspx.

64. Cho Mu-hyun, "South Korea to Invest $5b by 2020 in IoT and Smart Cars," ZDNet, March 25, 2015, http://www.zdnet.com/article/south-korea-to-invest-5b-by-2020-in-iot-and-smart-cars/.

65. James Lim, "South Korea Plans to Enforce Security of Internet of Things," Bloomberg BNA, November 2014, http://www.bna.com/south-korea-plans-n17179911433/.

66. "Korea's Global Commitment to Green Growth," World Ban, May 3, 2012, http://www.worldbank.org/en/news/feature/2012/05/09/Korea-s-Global-Commitment-to-Green-Growth.

67. "Fact Sheet: Administration Announces New "Smart Cities" Initiative to Help Communities Tackle Local Challenges and Improve Services," White House, September 14, 2015, https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help.

68. Ibid.

69. "Smart and Connected Communities Framework," Networking and Information technology Research and Development, November 25, 2014, https://www.nitrd.gov/sccc/materials/scccframework.pdf.

70. "A Strategy for American Innovation," White House, October 2015, http://www.manufacturing.gov/docs/strategy_for_american_innovation_october_2015.pdf.

71. "U.S. Department of Transportation Launches Smart City Challenge to Create a City of the Future," Department of Transportation, December 7, 2015, https://www.transportation.gov/briefing-room/us-department-transportation-launches-smart-city-challenge-create-city-future.

72. For example, the European Union's Horizon 2020 Lighthouse Projects consist of groups of cities developing smart city applications that have high market potential and are easy to replicate. "FAQ – Frequently Asked Questions WP 2015 for Horizon2020 call SCC 1 – 2015," European commission, 2015, https://ec.europa.eu/research/participants/portal/doc/call/h2020/h2020-scc-2015/1645153-faq_2015_v11_en.pdf.

73. Daniel Castro, "The Rise of Data Poverty in America," Center for Data Innovation, September 10, 2014, http://www2.datainnovation.org/2014-data-poverty.pdf.

74. Daniel Castro and Joshua New, “Accelerating Data Innovation: A Legislative Agenda for Congress,” Center for Data Innovation, May 11, 2015, http://www2.datainnovation.org/2015-data-innovation-agenda.pdf.

75. Daniel Castro and Joshua New, “10 Policy Principles for Unlocking the Potential of the Internet of Things,” Center for Data Innovation, December 4, 2015, http://www2.datainnovation.org/2014-iot-policy-principles.pdf.

76. Ibid.

77. Ibid.

ABOUT THE AUTHORS

Joshua New is a policy analyst at the Center for Data Innovation. He has a background in government affairs, policy, and communication. Prior to joining the Center for Data Innovation, Joshua graduated from American University with degrees in C.L.E.G. (Communication, Legal Institutions, Economics, and Government) and Public Communication. His research focuses on methods of promoting innovative and emerging technologies as a means of improving the economy and quality of life.

Daniel Castro is the director of the Center for Data Innovation and vice president of the Information Technology and Innovation Foundation. Mr. Castro writes and speaks on a variety of issues related to information technology and internet policy, including data, privacy, security, intellectual property, internet governance, e-government, and accessibility for people with disabilities. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading global think tank studying the intersection of data, technology, and public policy. With staff in Washington, DC and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The Center is a non-profit, non-partisan research institute proudly affiliated with the Information Technology and Innovation Foundation.

contact: info@datainnovation.org

datainnovation.org