Risk, Resilience, and Technological Complexity

Samuel Arbesman, PhD

Senior Fellow, Silicon Flatirons Center for Law, Technology, and Entrepreneurship at University of Colorado Law School; Scientist in Residence, Lux Capital

Our technological systems are growing more complicated and increasingly, so complex, that no one—including even the experts who have constructed these systems—fully understands them any longer. For example, software can exceed tens of millions of lines of computer code, technological infrastructure can be built upon computing hardware that is decades old, municipal transit systems are complex and interconnected enough to exceed human cognitive capacity, and technology projects can involve thousands of people over many years. There are several drivers of this growth in incomprehensibility over time, among them the increased interconnectivity of technologies and rapid technological growth, which leaves in its wake legacy code and legacy systems that are poorly understood. These forces of interconnectivity and the accretion of the new on top of the old lead to reduced understanding and increased technological risk, and in turn require new modes of thinking about these technologies and appropriate responses.

One response to grappling with risk in this realm of technological complexity is to try to construct these systems in a more resilient fashion, through the use of modularity and abstraction: building a system using reasonably distinct components whose interior construction can be ignored. However, while this can reduce risk of failure and promote understandability of these systems, too often the forces that lead us towards complexity are so strong that these are stopgap measures, at best.

Similarly, engineering a more resilient complex system can still lead to problems, such as these systems existing within a "robust, yet fragile" regime. "Robust, yet fragile" refers to systems that are robust to a wide variety of problems and stimuli (generally those situation that it is designed to handle), yet incredibly fragile to an unexpected failure. This can be seen in technological as well as biological systems, from aircraft to human beings, with the former susceptible to failure due to minute changes in computer chips and the latter susceptibility to small genetic changes, either at birth or later in life.

Therefore, in the face the often-inevitable robust yet fragile regime of complex technology, building a system for resilience must go hand in hand with two additional approaches: the practice of iteratively understanding the engineered complex system itself and proper risk communication.

Iterative understanding entails a new mode of grappling with our technologies: acting similar to biologists studying complex systems, rather than as engineers examining logical well-built constructions. Instead of viewing our technologies as well-understood systems from the outset, we must approach them with a scientist's curiosity, studying these massive, interconnected, and complicated constructions and slowly revealing their

behavior. This includes the study of bugs and glitches, behaviors that reveal the mismatch between how we thought the system might behave, and how it actually does. This process also involves the recognition that any understanding is necessarily tentative and incomplete. So whether one is actively involved in understanding a system or not, it is vital to internalize the inherent draft nature of one's conception of a technological system at any given point.

Risk communication involves accepting a certain amount of uncertainty in our understanding of a system's behavior (and takes the above perspective as a given), as well as the ability to effectively communicate this uncertainty. A striking example is from a 2006 press conference where the director of NASA provides a master class on such risk communication. Risk communication also involves a recognition that we often will have an inability to easily discover a single point of failure within a system, leaving us only able to point to the overall complexity and messiness of the system as the source of inevitable problems.

This presentation will briefly lay out the drivers of incomprehensible technological growth as well as the nature of robust yet fragile complex systems. It will then proceed to outlining a framework for iterative understanding as a means of mitigating risk, as well as the mental models and approaches required for proper risk communication.

PULSE SYMPOSIUM
Imagining the Legal Landscape: Technology and the Law in 2030

Giving Up On Cybersecurity

Kristen E. Eichensehr

ABSTRACT

Recent years have witnessed a dramatic increase in digital information and connected devices, but constant revelations about hacks make painfully clear that security has not kept pace. Societies today network first, and ask questions later.

This Essay argues that while digitization and networking will continue to accelerate, cybersecurity concerns will also prompt some strategic retreats from digital dependence. Individuals, businesses, and governments will "give up" on cybersecurity by either (1) adopting low-tech redundancies for high-tech capabilities or digital information, or (2) engaging in technological regression or arrest, foregoing capabilities that technology could provide because of concerns about cybersecurity risks. After cataloguing scattered examples of low-tech redundancy and technological regression or arrest that have occurred to date, the Essay critically evaluates how laws and regulations have fostered situations where giving up on cybersecurity is necessary. The Essay concludes by proposing ways that law can help to guide consideration of when to engage in low-tech redundancy or technological regression moving forward.

AUTHOR

Assistant Professor, UCLA School of Law. For helpful comments, I am grateful to participants in the Program on Understanding Law, Science, and Evidence (PULSE) conference on "Imagining the Legal Landscape: Technology and the Law in 2030." Thanks to Andrew Brown for excellent research assistance.

TABLE OF CONTENTS

INTRODUCTION 322
I. TWO WAYS TO GIVE UP ON CYBERSECURITY 323
  A. Giving Up as a Response to Security Concerns 324
  B. Giving Up So Far 327
    1. Low-Tech Redundancy 327
    2. Technological Regression or Arrest 330
II. LAW'S PUSH AND PULL 333
CONCLUSION 339

INTRODUCTION

Recent years have witnessed a dramatic escalation in digital information and connected devices. By some estimates, 90 percent of all data has been created in the last two years alone,[1] and the number of connected devices doubled between 2010 and 2015 and will double again or perhaps even quadruple by 2020.[2] The constant revelations about hacks of individuals, institutions, businesses, and governments, however, make painfully clear that security has not kept pace.[3] Societies today network first, and ask questions later.

This Essay argues that while the next fifteen years will undoubtedly see the predicted dramatic expansions of digitization and networked technologies, they will also be marked by instances where cybersecurity concerns prompt some strategic retreats from digital dependence. Individuals, businesses, and governments will "give up" on cybersecurity by either (1) adopting low-tech redundancies for high-tech capabilities or digital information, or (2) engaging in technological regression or arrest, choosing to forego capabilities that technology could provide because of security concerns. Scattered examples of giving up on cybersecurity are occurring now, and they will and should become more frequent going forward.

---

1. *See* Matthew Wall, *Big Data: Are You Ready for Blast-Off?*, BBC (Mar. 4, 2014), http://www.bbc.com/news/business-26383058 [https://perma.cc/FFZ9-SHLP]; *What is Big Data?*, IBM, http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html [https://perma.cc/H4Q9-XRAU].
2. *See, e.g.*, DAVE EVANS, CISCO, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011) (predicting that the number of connected devices will rise from 12.5 billion in 2010, to 25 billion in 2015, to 50 billion in 2020); INTEL, A GUIDE TO THE INTERNET OF THINGS: HOW BILLIONS OF ONLINE OBJECTS ARE MAKING THE WEB WISER, http://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png (predicting growth of connected objects from 2 billion in 2006, to 15 billion in 2015, to 200 billion in 2020); Philip N. Howard, *Sketching Out the Internet of Things Trendline*, BROOKINGS INST. (June 9, 2015), http://www.brookings.edu/blogs/techtank/posts/2015/06/9-future-of-iot-part-2 [https://perma.cc/A5RB-H6HT] (aggregating various predictions about the growth of the Internet of Things).
3. ADAM SEGAL, THE HACKED WORLD ORDER: HOW NATIONS FIGHT, TRADE, MANEUVER, AND MANIPULATE IN THE DIGITAL AGE 49 (2016) ("The history of cyberspace and cyber conflict is short, but the pace of history is rapidly accelerating. Whereas years or months once separated notable cyberattacks, now they come almost weekly, if not sometimes daily.").

Law often stands on the sidelines as technology charges ahead, intervening only after a significant delay, and that is certainly part of the story of the last fifteen years. But sometimes law has pushed the adoption of technologies and digitization of information in circumstances where it now appears that giving up on cybersecurity may be a better option. Law's role in pushing toward digital dependency suggests that it may also have a role to play in pulling back and guiding consideration of when to adopt low-tech redundancy or technological regression.

Part I of this Essay first defines "low-tech redundancy" and "technological regression or arrest." Part I.A explains how these concepts respond to concerns about the confidentiality, integrity, and availability of information. Part I.B catalogues examples of low-tech redundancy and technological regression or arrest that have occurred so far. Part II then critically evaluates how laws and regulations have fostered situations where giving up on cybersecurity is necessary and proposes ways that law can help to guide consideration of when to engage in low-tech redundancy or technological regression moving forward.

I. TWO WAYS TO GIVE UP ON CYBERSECURITY

The concept of "giving up" on cybersecurity captures two distinct phenomena spurred by cybersecurity concerns. The first is "low-tech redundancy." Low-tech redundancy involves deliberate decisions to retain low-tech or no-tech versions of capabilities or nondigital versions of content.[4] Think of this as knowing how to navigate without Google Maps' turn-by-turn instructions or as maintaining paper backups. Low-tech redundancy gives up on cybersecurity in the sense that it plans for the worst case scenario. It assumes that cybersecurity measures will fail and that digital files or technological capabilities will be

4. The strategy of low-tech redundancy is not necessarily limited to the cybersecurity context. The *New York Times* recently reported that to address security concerns posed by drones, European officials are considering using trained eagles to intercept drones that appear to threaten, for example, airports or public gatherings—"a low-tech solution for a high-tech problem." Stephen Castle, *Dutch Firm Trains Eagles to Take Down High-Tech Prey: Drones*, N.Y. TIMES (May 28, 2016), http://www.nytimes.com/2016/05/29/world/europe/drones-eagles.html?_r=2 [https://perma.cc/2MJV-A6RW] (quoting Sjoerd Hoogendoorn, the co-founder of the eagle program company, Guard From Above). The drone-hunting eagle program may be an example of low-tech redundancy: Dutch police detective chief superintendent Mark Wiebes explained to the *Times* that "subject to a final assessment," eagles are "likely to be deployed soon in the Netherlands, along with other measures to counter drones," such as "jamming drone signals." *Id.*

rendered inaccessible, inoperable, or untrustworthy. When that occurs, the low-tech alternatives ensure resilience.[5] They function as a failsafe, allowing continued operations and perhaps restoration of high-tech capabilities. Until cybersecurity fails, the high-tech and low-tech mechanisms proceed in parallel.[6]

The second phenomenon is "technological regression or arrest." Technological regression involves walking back from technological capabilities because of concern about the inability to properly secure the technology. Technological arrest is similar, capturing the deliberate decision not to proceed with developing a technical capacity because of security concerns. Technological arrest occurs when the security concerns are appreciated ex ante; technological regression occurs when the security implications are recognized only after the technology has been developed or deployed. Technological regression and arrest give up on cybersecurity in the sense that they assess that cybersecurity will fail and that the implications of that failure are sufficiently dire that the best course of action is to forego a technological capability entirely.

A. Giving Up as a Response to Security Concerns

Low-tech redundancy and technological regression and arrest respond to concerns about the confidentiality, integrity, and availability of data, which information security specialists often call the "CIA triad."[7]

A confidentiality problem involves access to data by individuals or entities that the owner of the data does not intend.[8] Data breaches are confidentiality problems: criminals hack a business's payment card system and obtain information, such as credit card numbers, that the business and individual

5. *See, e.g.*, Presidential Policy Directive/PPD-21--Critical Infrastructure Security and Resilience, WHITE HOUSE (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.cc/R8Z5-9CFR] ("The term 'resilience' means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.").

6. "High-tech" and "low-tech" are, of course, relative terms. As newer, more sophisticated technologies are developed, today's high-tech will become the future's low-tech. Today's cars are high tech as compared to the Model T, which was high-tech as compared to horse-drawn carriages, but today's cars will be low-tech when assessed against the future's driverless cars.

7. *See, e.g.*, P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR 35 (2014); Chad Perrin, *The CIA Triad*, TECHREPUBLIC (June 30, 2008, 8:13 AM), http://www.techrepublic.com/blog/it-security/the-cia-triad/ [https://perma.cc/C9AG-GAMA].

8. *See* SINGER & FRIEDMAN, *supra* note 7, at 35 (discussing confidentiality).

card holders intend to keep confidential. Intellectual property theft is another example of a confidentiality problem: hackers steal trade secrets, whose very intellectual property protection depends on their status as confidential information.

Availability problems occur when data or systems are not accessible to authorized users when they are supposed to be.[9] For example, in 2012 and early 2013, distributed denial of service (DDoS) attacks rendered the websites of numerous U.S. financial institutions inaccessible by flooding them with traffic and thereby preventing legitimate customers from accessing their accounts.[10] Data or technological capabilities could also be rendered unavailable due to physical damage to technical systems. Imagine a physical attack that disables or destroys satellites used for the Global Positioning System (GPS).

Integrity problems may be even more pernicious than confidentiality and availability problems. Data integrity problems involve unauthorized changes to data.[11] Integrity problems are particularly troubling because they are difficult to detect and once any integrity problem is discovered, it tends to cast doubt on the accuracy and reliability of all the other data on the system. The paranoia and time-consuming efforts to verify information that an integrity attack induces may be more damaging than the attack itself.[12] Although attacks that compromise the integrity of data have been rarer than the widespread confidentiality and availability problems,[13] they have occurred.

9. *See id.* (discussing availability).
10. *See* Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES (Jan. 8, 2013), http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0 [https://perma.cc/GJ39-7L98]; *see also* Indictment, United States v. Fathi, No. 16 Crim. 48 (S.D.N.Y. Mar. 24, 2016), https://www.justice.gov/usao-sdny/file/835061/download (charging seven hackers with ties to the Iranian government with crimes related to the distributed denial of service (DDoS) attacks on U.S. financial institutions).
11. *See* SINGER & FRIEDMAN, *supra* note 7, at 35 (discussing integrity).
12. *Id.* at 129 (arguing, in discussing attacks that compromise the integrity of military information, that "[o]nly a relatively small percentage of attacks would have to be successful in order to plant seeds of doubt in any information coming from a computer. Users' doubt would lead them to question and double-check everything from their orders to directions. . . . The impact could even go beyond the initial disruption. It could erode the trust in the very networks needed by modern military units to work together effectively . . . .").
13. James R. Clapper, Director of National Intelligence, *Worldwide Cyber Threats: Hearing Before the H. Permanent Select Comm. on Intelligence*, 114th Cong. 5 (2015), http://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf [https://perma.cc/Y8NA-X9S8] ("Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information; cyber espionage undermines

One significant example occurred with the alleged U.S. and Israeli cyberattack against Iranian nuclear facilities.[14] The operation, known as "Stuxnet," infected Iran's Natanz nuclear facility with malware and caused nuclear centrifuges to spin out of control, rendering them nonoperational.[15] In addition to the physical damage, the code recorded the centrifuges' normal operation, and then while the centrifuges spun out of control, it "sent signals to the Natanz control room indicating that everything downstairs was operating normally," a feature that one U.S. official called "the most brilliant part of the code."[16] According to the *New York Times*, the Iranians became "so distrustful of their own instruments that they . . . assigned people to sit in the plant and radio back what they saw," and they shut down entire "stands" of 164 centrifuges, looking for sabotage, when a few centrifuges failed.[17] U.S. officials have recently begun sounding warnings about integrity attacks.[18]

Low-tech redundancy primarily responds to concerns about availability and integrity. Governments, businesses, other organizations, and individuals may be forced to rely on redundant low-tech capabilities or paper backups

confidentiality, whereas denial-of-service operations and data deletion attacks undermine availability. In the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it. Decisionmaking by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.").

14. *See* David E. Sanger, *Obama Order Sped up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 [https://perma.cc/P3JA-QSAG].

15. *Id.*

16. *Id.*

17. *Id.* Another example of an integrity attack occurred in 2007 when Israel bombed a Syrian nuclear facility. A cyber attack on Syrian air defense computer systems caused Syrian radar operators to see false images—ones that did not reveal that Israeli planes had entered Syrian airspace—and "the air defense network never fired a shot." SINGER & FRIEDMAN, *supra* note 7, at 127.

18. *See, e.g.*, James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community: Hearing Before the S. Armed Serv. Comm.*, 114th Cong. 2 (2016), http://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf [https://perma.cc/UD82-5G42] ("Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decisionmaking, reduce trust in systems, or cause adverse physical effects."); Clapper, *supra* note 13, at 5 (warning about future attacks on data integrity); Katie Bo Williams, *Officials Worried Hackers Will Change Your Data, Not Steal It*, THE HILL (Sept. 27, 2015, 8:00 AM), http://thehill.com/policy/cybersecurity/254977-officials-worried-hackers-will-change-your-data-not-steal-it [https://perma.cc/PY6Z-AXEY] (reporting on congressional testimony by National Security Agency Director Michael Rogers warning about future cyberattacks aimed at undermining the integrity of data).

when high-tech systems are unavailable due to a cyberattack or when cyber intrusions undermine confidence in the reliability of high-tech methods or digital data. Technological regression and arrest also respond to integrity concerns, and they may be used to address confidentiality problems as well. In circumstances where, for example, the accurate functioning of a particular device is crucial, fear that the device cannot be secured—that its data will not remain confidential and that hackers could manipulate the data—may prompt a decision that the device should not be networked or that it should not be used at all.

B. Giving Up So Far

Scattered examples of both low-tech redundancy and technological regression and arrest exist now and will become increasingly common in the coming years.

1. Low-Tech Redundancy

One striking example of low-tech redundancy has emerged from the U.S. Naval Academy. After a nearly twenty-year hiatus, the Academy has resumed teaching cadets to navigate by the stars due to concern about vulnerabilities in the systems that the U.S. Navy currently uses for navigation.[19] The old-school navigation training will soon be expanded to enlisted personnel as well.[20] The advent of GPS drove the abandonment of celestial navigation training in the 1990s.[21] As Lieutenant Commander Ryan Rogers explained, the Navy "went away from celestial navigation because computers are great . . . . The problem is . . . there's no backup."[22] Knowledge about celestial navigation now serves as the backup. While experts have raised significant concerns about the security vulnerabilities of GPS,[23] "you can't hack a sextant."[24]

19. Andrea Peterson, *Cybersecurity Fears Are Making U.S. Sailors Learn to Navigate by the Stars Again*, WASH. POST (Oct. 14, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/10/14/cybersecurity-fears-are-making-u-s-sailors-learn-to-navigate-by-the-stars-again [http://perma.cc/6W3L-TCLL].
20. Tim Prudente, *Seeing Stars, Again: Naval Academy Reinstates Celestial Navigation*, CAPITAL GAZETTE (Oct. 12, 2015), http://www.capitalgazette.com/news/ph-ac-cn-celestial-navigation-1014-20151009-story.html [https://perma.cc/QUY9-44U3].
21. *Id.*
22. *Id.*
23. *See, e.g.*, Jose Pagliery, *GPS Satellite Networks Are Easy Targets for Hackers*, CNN (Aug. 4, 2015, 6:54 AM), http://money.cnn.com/2015/08/04/technology/hack-space-satellites [https://perma.cc/

Another example of a shift to nondigital redundancy involves voting machines. In the wake of the controversy about "hanging chads" in the 2000 presidential election, jurisdictions across the United States moved to modernize their voting equipment, including by adopting electronic voting machines or direct record electronic machines.[25] Almost immediately, computer scientists raised concerns about security vulnerabilities in electronic voting machines that could be exploited to tamper with election results.[26] Some jurisdictions responded to the security concerns by establishing low-tech redundancy: a paper record of each vote cast electronically. In February 2003, Santa Clara County, which includes Silicon Valley, became the first U.S. county to purchase electronic voting machines that produce a voter-verified paper receipt.[27] Later that same year, the California Secretary of State announced that beginning in July 2006, all electronic voting machines in California must produce a "voter verified paper audit trail."[28] Many other states have followed suit,[29] adopting laws requiring a paper backup for ballots cast

B7L7-74ST] (reporting on research that compromised a commercial GPS tracking network); Michael Peck, *The Pentagon Is Worried About Hacked GPS*, NAT'L INT. (Jan. 14, 2016), http://nationalinterest.org/feature/the-pentagon-worried-about-hacked-gps-14898 [https://perma.cc/W8AH-ULHF] (explaining the U.S. military's concerns about GPS jammers and physical attacks on GPS satellites and detailing the military's efforts to develop backup systems).

24. Prudente, *supra* note 20. For additional arguments about low-tech redundancy in the military context, see JACQUELYN SCHNEIDER, CTR. FOR NEW AMERICAN SECURITY, DIGITALLY-ENABLED WARFARE: THE CAPABILITY-VULNERABILITY PARADOX 9 (2016), http://www.cnas.org/sites/default/files/publications-pdf/CNASReport-DigitalWarfare-Final.pdf (arguing that the U.S. military should improve its resiliency by "acquiring technologies with both digital and manual capabilities" and increasing training for "back-up manual procedures").

25. For an overview of the post-2000 shift in voting equipment through 2005, see Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1717–41 (2005).

26. *See id.* at 1734–36.

27. *See Receipts Sought for Votes Cast Electronically*, N.Y. TIMES (Feb. 26, 2003), http://www.nytimes.com/2003/02/26/us/receipts-sought-for-votes-cast-electronically.html?rref=collection%2Ftimestopic%2FVoting%20Machines [https://perma.cc/RH3U-RPBH].

28. News Release, Sec'y of State Kevin Shelley, Secretary of State Kevin Shelley Announces Directives to Ensure Voter Confidence in Electronic Systems (Nov. 21, 2003), http://admin.cdn.sos.ca.gov/press-releases/prior/2003/03_106.pdf [https://perma.cc/3V22-E57E]. For an overview of the history of this shift in California, see ELECTIONLINE.ORG, BACK TO PAPER: A CASE STUDY 8–10 (2008), http://www.votetrustusa.org/pdfs/electionline/BacktoPaper.pdf [https://perma.cc/D8ZW-XTHM].

29. Some states have not engaged in low-tech redundancy (that is, paper backups), but instead have engaged in technological regression, abandoning electronic voting altogether in favor of a return to paper ballots. *See, e.g.*, ELECTIONLINE.ORG, *supra* note 28, at 4 (discussing New Mexico's return to paper ballots).

electronically.[30] Some states have been slow to respond to security concerns: Only in 2015 did Virginia decertify WINVote touchscreen voting machines, which suffered from numerous severe security flaws and produced no paper backups.[31] Other states still use vulnerable voting machines without paper backups.[32] Concerns about hacking of voting machines have become increasingly urgent in light of the alleged Russian hacking of the Democratic National Committee and the release of stolen information in an apparent attempt to influence the presidential election.[33]

A more quotidian example of low-tech redundancy is printing hard copies of important records or treasured photos. The last several years have seen a dramatic rise in ransomware—malicious software that encrypts a computer's hard drive and renders the information on it permanently inaccessible unless the victim pays the attackers (often in Bitcoin) to restore access.[34] Ransom-

30. *See* Cory Bennett, *States Ditch Electronic Voting Machines*, HILL (Nov. 2, 2014), http://thehill.com/policy/cybersecurity/222470-states-ditch-electronic-voting-machines [https://perma.cc/YV22-BPGN] (reporting that "[m]ore than 60 percent of states" have passed laws requiring paper trails for electronic votes); *see also The Verifier–Polling Place Equipment–Current*, VERIFIED VOTING, https://www.verifiedvoting.org/verifier [https://perma.cc/KC78-ZK9R] (showing various types of polling place equipment used by states).

31. *See* Kim Zetter, *Virginia Finally Drops America's 'Worst Voting Machines'*, WIRED (Aug. 17, 2015, 7:00 AM), http://www.wired.com/2015/08/virginia-finally-drops-americas-worst-voting-machines [https://perma.cc/P3S7-9MYX] (cataloguing numerous security problems with the machines, including insecure encryption, default passwords, and software that had not been patched since 2005).

32. *See* Grant Gross, *A Hackable Election? 5 Things To Know about E-Voting*, COMPUTERWORLD (July 22, 2016, 8:57 AM), http://www.computerworld.com/article/3099018/security/ahackable-election-5-things-to-know-about-e-voting.html [https://perma.cc/XAU4-F8GQ] (highlighting security concerns stemming from some states' continued use of electronic voting machines without paper backups).

33. Bruce Schneier, *By November, Russian Hackers Could Target Voting Machines*, WASH. POST (July 27, 2016), https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/ [https://perma.cc/48BE-NCAL] ("Longer term, we need to return to election systems that are secure from manipulation. This means voting machines with voter-verified paper audit trails . . . . I know it's slower and less convenient to stick to the old-fashioned way, but the security risks are simply too great."). For details on the evidence that Russia is responsible for the Democratic National Committee hack, see, for example, David E. Sanger & Eric Schmitt, *Spy Agency Consensus Grows That Russia Hacked D.N.C.*, N.Y. TIMES (July 26, 2016), http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html?_r=0 [https://perma.cc/G5PU-V83S]; Patrick Tucker, *How Putin Weaponized Wikileaks to Influence the Election of an American President*, DEFENSEONE (July 24, 2016), http://www.defenseone.com/technology/2016/07/how-putin-weaponized-wikileaks-influence-election-american-president/130163 [https://perma.cc/XV4E-ZYZV].

34. *Ransomware on the Rise: FBI and Partners Working to Combat This Cyber Threat*, FBI (Jan. 20, 2015), https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise [https://perma.cc/3QUG-C7KM]; Kim Zetter, *Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the*

ware strikes not just individuals, but increasingly businesses, including hospitals,[35] which have paid to restore access to electronic systems.[36] Even Vint Cerf—one of the "Fathers of the Internet" and currently Google's "Chief Internet Evangelist"[37]—exhorted people to print important items. In a 2015 speech, he warned, "If there are pictures that you really really care about then creating a physical instance is probably a good idea. Print them out, literally."[38] The motivation for Cerf's warning was not security so much as the march of technology and the possibility that future technology will lack the backwards compatibility necessary to read earlier file formats, effectively creating a digital "Dark Age" of inaccessible data.[39] But the basic point is the same: low-tech redundancy in the form of paper copies of digital files as a way to mitigate the risks of inaccessibility or compromised integrity of digital files.

2. Technological Regression or Arrest

Examples of technological regression or arrest also run the gamut from issues of national security to corporate and consumer contexts.

In the wake of Edward Snowden's revelations, Russia's Federal Guard Service (FSO), which protects high-ranking Russian officials, reportedly ordered typewriters in an attempt to keep sensitive communications from being

Rise, WIRED (Sept. 17, 2015, 4:08 PM), http://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise [https://perma.cc/K5PV-YA5D].

35. John Woodrow Cox et al., *Virus Infects MedStar Health System's Computers, Forcing an Online Shutdown*, WASH. POST (Mar. 28, 2016), https://www.washingtonpost.com/local/virus-infects-medstar-health-systems-computers-hospital-officials-say/2016/03/28/480f7d66-f515-11e5-a3ce-f06b5ba21f33_story.html [https://perma.cc/K3DD-JS2L] (noting that the infection of the Medstar computer system forced "hospital staff . . . to revert to seldom-used paper charts and records").

36. *See* Sean Gallagher, *Patients Diverted to Other Hospitals After Ransomware Locks Down Key Software*, ARS TECHNICA (Feb. 17, 2016), http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack [https://perma.cc/PA55-HPU4]; Richard Winton, *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating*, L.A. TIMES (Feb. 18, 2016), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html [https://perma.cc/J68Q-UHPN].

37. *Vinton G. Cerf*, RESEARCH AT GOOGLE, http://research.google.com/pubs/author32412.html [https://perma.cc/ZKL7-6TU3].

38. Sarah Knapton, *Print out Digital Photos or Risk Losing Them, Google Boss Warns*, TELEGRAPH (Feb. 13, 2015, 11:06 AM), http://www.telegraph.co.uk/news/science/science-news/11410506/Print-out-digital-photos-or-risk-losing-them-Google-boss-warns.html [https://perma.cc/FD89-BAVJ] (quoting Vinton Cerf).

39. *Id.*

electronically surveilled.[40] An FSO source explained to the Russian newspaper *Izvestiya* that "the practice of creating paper documents will expand."[41] The technological regression may not be limited to Russia. A German member of parliament who heads a parliamentary inquiry into National Security Agency activities said in an interview that "he and his colleagues were seriously thinking of ditching email completely," and when asked whether they considered typewriters, he replied, "As a matter of fact, we have—and not elec-electronic models either."[42]

Technological regression goes beyond communications technologies. The rapid increase of a wide range of networked devices as part of the "Internet of Things" is prompting cybersecurity concerns related to everything from medical devices[43] to children's toys[44] to cars.[45] One example of technological regression came to light in a 2013 *60 Minutes* interview with former Vice President Dick Cheney. Cheney disclosed that "his doctor ordered the wireless functionality of his heart implant disabled due to fears it might be hacked in an assassination attempt."[46] Cheney's revelation shows technological regres-

40. Miriam Elder, *Russian Guard Service Reverts to Typewriters After NSA Leaks*, GUARDIAN (July 11, 2013), http://www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks [https://perma.cc/H5UW-KNF6].

41. *Id.* (quoting a source inside the Federal Guard Service).

42. Philip Oltermann, *Germany 'May Revert to Typewriters' to Counter Hi-Tech Espionage*, GUARDIAN (July 15, 2014, 1:04 PM), http://www.theguardian.com/world/2014/jul/15/germany-typewriters-espionage-nsa-spying-surveillance [https://perma.cc/J6NJ-SE4F] (quoting Patrick Sensburg).

43. *See, e.g.*, News Release, U.S. Food & Drug Admin., FDA Outlines Cybersecurity Recommendations for Medical Device Manufacturers (Jan. 15, 2016), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm [https://perma.cc/LX7S-GYMD]; *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, U.S. FOOD & DRUG ADMIN., (July 31, 2015), http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm [https:// perma.cc/GL48-ZS6S] (recommending that hospitals cease using the Hospira Symbiq Infusion System because cybersecurity vulnerabilities allow the pump to be remotely accessed and thus allow unauthorized users to change the dosage the pump administers).

44. *See, e.g.*, Whitney Meers, *Hello Barbie, Goodbye Privacy? Hacker Raises Security Concerns*, HUFFINGTON POST (Nov. 30, 2015, 4:45 PM), http://www.huffingtonpost.com/entry/hello-barbie-security-concerns_us_565c4921e4b072e9d1c24d22 [https://perma.cc/FU7H-LH97].

45. *See, e.g.*, Sean Gallagher, *Highway to Hack: Why We're Just at the Beginning of the Auto-Hacking Era*, ARS TECHNICA (Aug. 23, 2015, 8:00 AM), http://arstechnica.com/security/2015/08/highway-to-hack-why-were-just-at-the-beginning-of-the-auto-hacking-era [https://perma.cc/39B6-XX3R].

46. Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart [https://perma.cc/8FE7-MAVS].

sion for one medical device, but regression on a broader scale might occur as a result of regulation or in the wake of an incident of patient harm from hacking of a medical device.

Similarly, consumers may drive demand for regression in some instances. For example, German researchers in March 2016 released a study showing that twenty-four different models of cars from nineteen manufacturers are vulnerable to a "radio 'amplification attack' that silently extends the range of unwitting drivers' wireless key fobs to open cars and even start their ignitions," greatly facilitating car theft.[47] Although consumers undoubtedly enjoy the convenience of keyless entry and ignition, cybersecurity concerns might push at least well-informed consumers to demand old school, physical car keys.[48]

While technological regression involves undoing a technological capability in response to security concerns, examples of technological arrest are characterized by a deliberate decision not to go high-tech—not to network a device, not to create a digital file—due to security concerns.[49] For example, in the wake of the 2014 cyberattack on Sony Pictures, Hollywood studios are working to improve their cybersecurity.[50] Some of the techniques involve using more sophisticated technology, like encryption, to secure digital copies of movie scripts, but other techniques involve technological arrest. According to reports, "[t]he most-coveted scripts are still locked in briefcases and ac-

47. Andy Greenberg, *Radio Attack Lets Hackers Steal 24 Different Car Models*, WIRED (Mar. 21, 2016, 10:33 AM), http://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack [https://perma.cc/Q6S6-ZZWM].

48. As just one example, in response to an article about the radio amplification attacks, Shawn Henry, the president of cybersecurity firm Crowdstrike Services, tweeted, "My ignition key worked pretty well for the past 30 years. Maybe we don't need to incorporate tech into EVERYTHING?!" Shawn Henry (@Shawn365Henry), TWITTER (Mar. 23, 2016, 8:36 AM), https://twitter.com/Shawn365Henry/status/712619038531198976 [https://perma.cc/Z6TQ-AM32].

49. *See, e.g.*, Darren Samuelsohn, *GOP Shuns Electronic Ballots at Open Convention*, POLITICO (May 1, 2016, 4:56 PM), http://www.politico.com/story/2016/05/gop-convention-ballots-technology-222472 [https://perma.cc/7VAZ-PH5W] (reporting that senior Republican party officials "rul[ed] out a change to convention bylaws that would allow for electronic voting on" presidential and vice presidential nominees due in part to concerns about hacking); Schneier, *supra* note 33 (arguing against Internet voting due to cybersecurity concerns).

50. Nicole Perlroth, *Secrecy on the Set: Hollywood Embraces Digital Security*, N.Y. TIMES (Mar. 29, 2015), http://www.nytimes.com/2015/03/30/technology/secrecy-on-the-set-hollywood-embraces-digital-security.html?_r=1 [https://perma.cc/8HJB-C4JV].

companied by bodyguards whose sole job is to ensure they don't end up in the wrong hands."[51]

The Apple-versus-FBI dispute over access to the iPhone of one of the San Bernardino shooters provides another technological arrest example. In February 2016, a magistrate judge in the Central District of California ordered Apple to assist the FBI in accessing the iPhone by writing software that would, among other things, override a feature of the phone that caused it to auto-erase after ten incorrect attempts to guess its passcode.[52] Apple raised many legal and policy objections to the court's order,[53] and one is essentially an argument for technological arrest.[54] Specifically, Apple argued that the court's order would require "Apple to design, create, test, and validate a new operating system that does not exist, and that Apple believes—with overwhelming support from the technology community and security experts—is too dangerous to create."[55] Apple cited the risks that the code would be leaked or stolen by hackers as a reason for its refusal to write the code in the first place.[56]

II. LAW'S PUSH AND PULL

Numerous drivers have pushed the digital revolution and increased dependence on technology. Businesses and governments adopt technology because it improves efficiency and gives them new capabilities. Customers

51. *Id.*
52. Order Compelling Apple, Inc. to Assist Agents in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M (C.D. Cal. Feb. 16, 2016), https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-Magistrate-Order.pdf.
53. *See* Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 14-35, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. CM 16-10 (SP) (C.D. Cal. Feb. 25, 2016) [hereinafter Apple Brief], https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-Apple-Motion-to-Vacate-With-Declarations.pdf.
54. *Id.* at 2.
55. Apple Inc.'s Reply to Government's Opposition to Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search at 16, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. CM 16-10 (SP) (C.D. Cal. Mar. 15, 2016) [hereinafter Apple Reply Brief], https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-CDCal-Apple-Reply.pdf; *see also* Apple Brief, *supra* note 53, at 2 (arguing that the court's order "compels Apple to create a new operating system—effectively a 'back door' to the iPhone—that Apple believes is too dangerous to build").
56. Apple Reply Brief, *supra* note 55, at 19–20.

seeking convenience or just the coolest new device form a vast market for high-tech gadgets, mobile phones, and tech-dependent services. Companies seeking to capture pieces of these highly lucrative markets rush products onto (often digital) shelves, fiercely competing with similarly situated firms. Because of these interests, adoption of technologies often occurs before full consideration of their security implications. As the examples of low-tech redundancy and technological regression and arrest show, demands for efficiency, convenience, and greater capabilities often lead to adoption first, careful consideration later.

Law and regulation are at least complicit in this situation. Law often lags behind technology, only belatedly catching up to a technology's implications and uses after the technology has been deployed. But in some circumstances, laws and regulations are partially to blame for creating the situation in which dependence on technology outpaces efforts to secure it. Government entities sometimes adopt technologies themselves without fully considering security problems. Consider, for example, the electronic voting machines that jurisdictions across the United States approved and purchased without appreciating that they could be hacked and compromise the integrity of elections and voter confidence in the electoral process. Another example is the federal government's adoption of electronic processing of security clearance investigations, including electronic security clearance forms and digital fingerprints.[57] This information was stored in a centralized database that China compromised in last year's hack of the Office of Personnel Management.[58] In the

57. *See Security Clearance Reform: Moving Forward on Modernization: Before the Subcomm. on Oversight of Gov't Mgmt., the Fed. Workforce, and the District of Columbia, U.S. S. Comm. on Homeland Sec. & Governmental Affairs*, 111th Cong. (Sept. 15, 2009) (statement of John Berry, Director, U.S. Office of Personnel Management), https://www.opm.gov/news/testimony/111th-congress/security-clearance-reform-moving-forward-on-modernization-september [https://perma.cc/C59N-8STQ] (describing federal government agencies' adoption of electronic background investigation forms and digital fingerprint records as part of security clearance investigations).

58. *See* David E. Sanger, *Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says*, N.Y. TIMES (Sept. 23, 2015), http://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html?_r=0 [https://perma.cc/G85G-J3GP] (reporting that the Office of Personnel Management hack, attributed to China, compromised personal information of 22 million people and fingerprints of 5.6 million U.S. government employees).

wake of the intrusion, the government reverted to hard copy security clearance applications, at least temporarily.[59]

Sometimes the government has also mandated or provided incentives for other entities to adopt technologies. One example is digitization of medical records. Passed as part of the American Recovery and Reinvestment Act of 2009,[60] the Health Information Technology for Economic and Clinical Health (HITECH) Act[61] "established incentive programs for eligible hospitals and professionals adopting and meaningfully using certified electronic health record . . . technology."[62] Regulations issued under the Act provide for incentive payments under Medicare and Medicaid to health care providers that meaningfully use electronic health records, but the regulations also provide for decreased Medicare payments to providers who fail to meet electronic health record standards.[63] Although these laws were a well-intentioned attempt to improve efficiency and patient safety,[64] they have also pushed hospitals toward dependence on digital records that are now subject to hacks and ransomware attacks.[65]

On the upside, the fact that laws and regulations are partly responsible for pushing toward digital dependency suggests that they may also be able to play a constructive role in pulling back from it in narrowly tailored and strategic

59. Billy Mitchell, *OPM Reverts to Paper Forms During e-QIP Suspension*, FEDSCOOP (July 6, 2015, 5:20 PM), http://fedscoop.com/opm-oks-paper-clearance-forms-during-e-qip-suspension [https://perma.cc/NE8H-QLY5].

60. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

61. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, §§ 13001–13424, 123 Stat. 226 (2009).

62. Frank Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, 72 MD. L. REV. 682, 708–09 (2013). For an overview of the incentive programs, see *Medicare and Medicaid EHR Incentive Program Basics*, CTRS FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Basics.html [https://perma.cc/5MSN-LXXC].

63. Medicare and Medicaid Programs; Electronic Health Record Incentive Programs—Stage 3 and Modifications to Meaningful Use in 2015 Through 2017, 80 Fed. Reg. 62,761, 62,765 (Oct. 16, 2015) (to be codified at 42 C.F.R. pts. 412 and 495).

64. *See* President Barack Obama & Vice President Joe Biden, *Remarks by the President and Vice President at Signing of the American Recovery and Reinvestment Act*, WHITE HOUSE (Feb. 17, 2009), https://www.whitehouse.gov/the-press-office/remarks-president-and-vice-president-signing-american-recovery-and-reinvestment-act [https://perma.cc/F5YW-4UWC] (explaining the American Recovery and Reinvestment Act as "an investment that will take the long overdue step of computerizing America's medical records to reduce the duplication and waste that costs billions of health care dollars, and medical errors that cost thousands of lives each year").

65. *See supra* note 35 and accompanying text.

ways. Setting aside legal regulation to improve cybersecurity and the debates that accompany it, law and regulations could help to require or incentivize giving up on cybersecurity via low-tech redundancy or technological regression.

Examples of laws mandating low-tech redundancy are easy to imagine and in some cases already exist. For example, the same jurisdictions that passed laws or ordinances requiring electronic voting could just as easily require all voting machines to produce a paper backup.[66] Similarly, the laws and regulations that incentivize digitization of medical records could mandate or provide incentives for health care providers to produce periodic paper backups of at least some documents, for instance, patient allergy information. Laws could similarly incentivize individuals to maintain low-tech capabilities. Ownership of self-driving cars could be contingent on the owner obtaining a driver's license for conventional cars. None of these legal moves would abandon the advantages of digitization or new technology, but they would preserve low-tech redundancy that could be drawn upon if the high-tech options were destroyed, made inaccessible, or rendered untrustworthy.

Laws and regulations could similarly foster consideration of technological regression. For industries that are already regulated, agencies could require a risk assessment for networked devices that would specifically evaluate whether the benefits of the networking outweigh the security risks. Forcing explicit consideration of cybersecurity risk could push companies toward technological regression. Examples in this category might be the Food and Drug Administration's regulation of medical devices,[67] and the National Highway Traffic Safety Administration's regulation of motor vehicle safety.[68]

In addition to federal government agencies, state laws and regulations might provide other avenues for prompting companies to consider technological regression explicitly. States and state attorneys general in particular have been active in protecting consumer privacy through mechanisms such as state data breach notification statutes.[69] Many have consumer protection-focused mandates

66. *See supra* notes 28 and 30 and accompanying text.
67. *See Overview of Device Regulation*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview [https://perma.cc/C4PJ-M4NK].
68. *See* Federal Motor Vehicle Safety Standards, 49 C.F.R. § 571 (2015).
69. *See, e.g.*, *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/BUQ2-NE33] (compiling state data breach notification laws).

as well.[70] States might issue guidance or provide incentives or mandates for consumer product companies that sell networked devices to consider device security. They might even require product manufacturers to preserve the ability to de-network consumer products and to disclose to consumers how to de-link devices from the Internet. To be sure, such a requirement would pose practical challenges, including how to provide the information to consumers and whether the information on de-linking the device could be communicated in a sufficiently understandable way for the average consumer to follow the instructions if he or she chose to do so.[71]

Another way law could incentivize consideration of low-tech redundancy or technological regression is by incorporating such consideration into the standard of care for what constitutes reasonable cybersecurity. For the last decade,[72] the Federal Trade Commission (FTC) has brought administrative actions against companies that demonstrate weak cybersecurity with respect to customer data. The FTC actions are based on Section 5 of the Federal Trade Commission Act's prohibition on "unfair or deceptive acts or practices in or affecting commerce."[73] The Commission's authority to regulate inadequate cybersecurity pursuant to Section 5 received a significant boost in 2015 when the Third Circuit Court of Appeals rejected a challenge to the FTC's authority by Wyndham Hotels, which was the subject of an FTC enforcement action after three data breaches compromised credit card information of more than 619,000 customers and resulted in "at least $10.6 million" in fraudulent charges.[74] Most of the FTC's more than fifty enforcement actions

70. *See, e.g.*, *Protecting Consumers*, ST. CAL. DEP'T JUST.: OFF. ATT'Y GEN., https://oag.ca.gov/consumers [https://perma.cc/7GZG-3YHN]; *Consumer Protection*, ATT'Y GEN. TEX. KEN PAXTON, https://texasattorneygeneral.gov/cpd/consumer-protection [https://perma.cc/RS9A-3BDD]; *Consumer Protection*, ATT'Y GEN. MARK R. HERRING, http://www.oag.state.va.us/citizen-resources/consumer-protection [https://perma.cc/5JEG-ZWGU].

71. Some of these challenges occur with respect to privacy policies for connected devices, which do not even attempt to convey technical information about how to alter a device's functions. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 140–43 (2014).

72. For an overview of the FTC's history of data security enforcement actions, see GINA STEVENS, CONG. RESEARCH SERV., THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 7–8 (2014), http://fas.org/sgp/crs/misc/R43723.pdf (tracing the history of FTC data security enforcement actions beginning in 2006).

73. 15 U.S.C. § 45(a) (2012).

74. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 242 (3d Cir. 2015).

have resulted in settlements,[75] and the settlements focus on companies' failure to employ basic cybersecurity practices, such as requiring secure passwords and keeping software updated.[76]

In the future, the FTC's understanding of what counts as "unfair" practices could evolve to include maintenance of low-tech redundancy and consideration of technological regression. For example, in response to a wave of attacks that renders customer services unavailable—think inability to access personal health tracking data or travel reservations—the Commission could come to regard a company's failure to maintain low-tech redundancy in the form of paper backups or other means for continued customer access to data as an unfair practice. In other words, the failure to maintain continuity of operations during a cyberattack—including through low-tech redundancy—could be understood to be an unreasonable cybersecurity practice and one that is unfair to consumers.

The FTC might also address technological regression as an extension of existing concerns about unnecessary collection of consumers' data. The FTC already advises businesses to avoid collecting personal information they do not need and to retain consumers' personal data only for as long as there is a legitimate business need for the data.[77] The FTC has highlighted these "data minimization" best practices specifically in connection with the Internet of Things.[78] The Commission gave an example of a wearable device that tracks a health condition and has the ability to monitor the wearer's physical location.[79] The Commission suggests that until the company needs the geolocation information for a future product feature that would allow users to find medical care near their location, the company should not collect the location data.[80] The FTC's example could be understood to push for consideration of technological regression: The wearable technology company would turn off a feature of the device absent a business need that would justify collecting data

75. FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS: LESSONS LEARNED FROM FTC CASES 1 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
76. *Id.* at 4–5, 12.
77. *Id.* at 2.
78. FTC STAFF REP., INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 33–39 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
79. *Id.* at 36.
80. *Id.*

and thereby putting it at risk of compromise.[81] It is worth emphasizing that under the FTC's current approach, the existence of a business need for data appears sufficient to justify its collection. A full embrace of consideration of technological regression, on the other hand, might change the analysis so that the mere existence of a business need for data is not necessarily sufficient; rather the reasonableness of a company's practices could turn on a balancing between the cybersecurity risks of a technology and the benefits it provides to consumers.

CONCLUSION

The website of "I Am The Cavalry"—a "grassroots organization" focused on the intersection of computer security and public safety[82]—notes that "[a]s the question around technology is less-and-less 'can we do this' we must more-and-more be asking 'should we do this.'"[83] As the examples of low-tech redundancy and technological regression suggest, sometimes that answer should be "no." Going forward, legal institutions from executives to legislatures to regulatory agencies should consider whether low-tech redundancy should be maintained alongside high-tech capabilities and digital data and whether in limited circumstances, the convenience, efficiency, and other benefits of a technology might not overcome the cybersecurity risks that it poses.

Discussions of technological progression don't often end in discussions of technological regression. But maybe they should.

---

81. FED. TRADE COMM'N, *supra* note 75, at 2 (highlighting security risk to unnecessarily collected and retained data); FTC STAFF REP., *supra* note 78, at 34–35 (explaining that collection and retention of unnecessary data increases security risk because "[l]arger data stores present a more attractive target for data thieves").

82. *Executive Summary*, I AM THE CAVALRY, https://www.iamthecavalry.org/about/overview [https://perma.cc/8SCE-BPBC].

83. *Id.*

PRELIMINARY DRAFT: CITE WITH CAUTION
Comments welcome at wnp@umich.edu

RISK AND RESILIENCE IN HEALTH DATA INFRASTRUCTURE

W. Nicholson Price II, PhD [*]

Today's health system runs on data. Patients and doctors complain about the proportion of time during a patient appointment that is spent entering data into the doctor's computer, but this has become the new normal. Data are supposed to help improve care for individual patients, to increase the efficiency of the system as a whole, and to provide the basis for future innovation in care.

However, for a system that generates and requires so much data, the health care system is surprisingly bad at maintaining, connecting, and using those data. In the easy cases, it works. If a patient stays with the same primary care physician, coordinates all care through that physician, goes to the same pharmacy, the same hospital, and the same labs, and uses the same insurer, that patient's records may—*may*—be integrated into a single comprehensive medical record that tracks the patient's health over time. But patients don't behave like this most of the time. Patients move between providers, pick up drugs while traveling, switch insurers as they change jobs (or lose them), see different specialists, and generally vary the parameters of their care. And the health data system does a poor job accounting for this fragmentation of care, resulting in fragmented data.

Fragmented data create risks to patients and to the system as a whole. At the patient level, fragmentation creates risks in care, where information necessary for effective care is either not available or incorrect. Fragmentation also creates risks for patient privacy, as a result of the needs to haphazardly share data across different health actors. At the systemic level, data fragmentation hinders efforts to make the system more efficient as a whole, because putative optimizers only see a fragment of the picture. It also slows innovation in health, especially big-data driven modern initiatives that rely on large, high-quality datasets for their power and accuracy.

Efforts to combat data fragmentation would benefit by considering the idea of health data infrastructure. Most obviously, that would be infrastructure

[*] Assistant Professor of Law, University of Michigan Law School. JD, 2011, Columbia University School of Law. PhD (Biological Sciences), 2010, Columbia University Graduate School of Arts and Sciences. For helpful conversations and feedback, I wish to thank Ana Bracic, Rebecca Eisenberg, and the participants in the Silicon Flatirons Digital Broadband Migration Conference. All errors are my own.

both *for* health data—that is, infrastructure on which health data can be stored and transmitted. But it should also be an infrastructure *of* health data—that is, a platform of shared data on which to base further efforts to increase the efficiency or quality of care.

This essay proceeds in three Parts. Part I describes the landscape of health data today, including potential benefits of the collection of health data and the reasons for fragmentation which limits those benefits. Part II describes the risks of a fragmented health data system. Part III sketches the basics of how an infrastructure vision for and of health data might look.

I. HEALTH DATA TODAY

The health system generates a blizzard of data at an increasing rate. From the paper records of prior practice, providers have largely moved to use electronic health records (also called electronic medical records).[1] New forms of data are proliferating to fill those records, including the reports of traditional medical encounters, high-volume diagnostic tests such as genetic sequencing and analysis, prescription records, and others.[2]

A. Potential Benefits

These data are collected for a reason; they are supposed to create substantial benefits for patients, providers, and for the health system as a whole. Ideally, they should lead to improved care for individual patients as integrated medical records prevent easily avoidable medical error and allow a broader picture of the patient's overall health.[3] They should enable more efficient care by reducing the costs of coordination, should decrease costs, and should even enable more effective and efficient billing by insurers. On a slightly more systemic level, many health care reforms rely on the ability to measure care precisely—for instance, to observe whether patients are treated according to approved procedures or are readmitted to hospitals too

---

[1] The move to electronic health records was not accidental. A substantial sum was made available for providers to shift to electronic records HITECH Act, passed as part of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (Feb. 17, 2009) (ARRA), Div. A, Title XIII, Div. B, Title IV. *See* Rebecca S. Eisenberg & W. Nicholson Price II, *Promoting Health Innovation on the Demand Side*, __ J.L. & BIOSCIENCES __ (2017). As a powerful counterpart, penalties are imposed on entities failing to shift to and meaningfully use electronic records by established deadlines. *See id.* at __; Centers for Medicare and Medicaid Services, *Medicare and Medicaid EHR Incentive Program Basics*, Jan. 12, 2016, https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/basics.html.

[2] *See* Eisenberg & Price, *supra* note 1, at __.

[3] *See*, *e.g.*, James R Broughman & Ronald C Chen, *Using Big Data for Quality Assessment in Oncology*, 5 J. COMP. EFF. RES. 309 (2016).

frequently.[4] Health data enable the imposition of sanctions or the provision of incentives to try to shape health care in productive ways.[5]

Data are also supposed to enable us to draw more nuanced and useful information from the health system. Insurers and others have used information about actual patient experience in the health system to demonstrate that certain drugs are less safe than expected,[6] that some treatments may be more cost-effective at providing the same benefit,[7] that some patients gain more benefit from a particular treatment than others,[8] or that a drug should be moved from prescription-only to over-the-counter status.[9] Recently, FDA has even gained the statutory authority to use this type of real-world evidence to approve new indications for drugs.[10] More broadly, health data can potentially lead to advances in precision medicine. Precision medicine, the scientific tailoring of medical treatment to reflect individual patient variation, requires knowing how different patients respond to different forms of treatment.[11] Some of this knowledge can be generated by classical hypothesis-driven scientific and clinical studies, but other advances, including those relying on machine-learning and other forms of datamining, rely on large sets of existing health data.[12]

Overall, health data offer substantial promise for improving health care,

---

[4] *See, e.g.*, Broughman & Chen, *supra* note 3.

[5] *See* Medicare Access and CHIP Reauthorization Act of 2015 (MACRA), Pub. L. No. 114-10, 129 Stat. 87, § 102 (requiring a plan to develop data-based measures for physician and hospital performance), § 101 (creating payment incentive structures using those measures).

[6] *See* Eisenberg & Price, *supra* note 1, at __ (discussing the identification of toxic side effects of the painkiller Vioxx by Kaiser Permanente, which analyzed patient records in its integrated health system and found higher rates of heart attacks among patients taking Vioxx than among patients taking other similar drugs).

[7] *See id.* § I.C.2 (describing cost-effectiveness research and the use of observational studies of patient data to perform such research).

[8] *See id.* (describing comparative-effectiveness research).

[9] *Id.* at § I.A.1 (describing a petition filed by Blue Cross of California (later Wellpoint) to take certain antihistamines, including Claritin, over-the-counter).

[10] *See* 21st Century CURES Act, Pub. L. No. 114-255, § 3022 (requiring FDA to "establish a program to evaluate the potential use of real world evidence" for the approval of new indications for an already-approved drug or to fulfill post-approval study or surveillance requirements). This provision has been the subject of considerable criticism. *See, e.g.*, Jerry Avorn & Aaron S. Kesselheim, *The 21st Century Cures Act — Will It Take Us Back in Time?*, 372 N. ENGL. J. MED. 2473 (2015).

[11] Laura K. Wiley et al., *Harnessing next-Generation Informatics for Personalizing Medicine: A Report from AMIA's 2014 Health Policy Invitational Meeting*, 23 J. AM. MED. INFORM. ASSOC. 413 (2016); Marc L Berger et al., *Opportunities and Challenges in Leveraging Electronic Health Record Data in Oncology*, 12 FUTURE ONCOL. 1261 (2016).

[12] *See* W. Nicholson Price II, *Black-Box Medicine,* 28 HARV. J.L. & TECH. 419, 429–34, 437–39 (2015) (describing the big data potential and requirements of next-generation black-box medicine).

both in terms of near-term patient-specific benefits and in terms of later innovations to improve the health system. Unfortunately, these benefits have been slow to materialize. At least in part, this slowness has resulted from the fragmentation of health data.[13]

B. Fragmentation

Why are health data today so fragmented? There are at least three linked reasons. First, and most obviously, care itself is fragmented. Second, and related, competition between entities in the health system reduces incentives to connect and link data. Third and finally, legal barriers to information sharing, especially the Health Insurance Portability and Accountability Act, make it hard to link data.

1. Fragmented care

The key underlying cause of health data fragmentation is that health care is itself fragmented, and with it the generation and storage of health data.[14] Patients see different doctors at different times, visit different drugstores, change insurers, and in other ways participate in an inherently fragmented health system.[15] Correspondingly, hospitals, doctors, insurers, and pharmacies all keep their own records. These records are generated for different purposes and may use different terms or code different information.[16] For instance, insurance claims records are principally generated for the purpose of payment; accordingly, they lack some forms of care data and may potentially be skewed.[17] The relevant information about patient care is thus spread among different actors in the health care system, in different forms.

Health data are not only generated in the course of health care. Research companies like 23andMe collect substantial health information[18] but are not

---

[13] The fragmentation of health data is certainly not the only cause for the delay in realizing benefits of health data innovation. Some actors lack the right incentives to actively move toward the highest-quality, most efficient care. *See*, *e.g.*, Eisenberg & Price, *supra* note 1, at __ (discussing the problematic incentives for health insurers and for drug manufacturers); David Orentlicher, *Paying Physicians More to Do Less: Financial Incentives to Limit Care*, 30 UNIV. RICHMOND L. REV. 155 (1996) (discussing the incentives of doctors to provide more care than necessary). Technological hurdles also play a role. *See* Eisenberg & Price, *supra* note 1, at § I.D. And even once innovative information is generated, getting health care providers to implement the new knowledge can be challenging. *Id.* at § II.B.

[14] *See*, *e.g.*, Alan M. Garber & Jonathan Skinner, *Is American Health Care Uniquely Inefficient*, 22 J. ECON. PERSP. 27 (2008) (noting popular wisdom that the American health care system is exceptionally fragmented).

[15] *See* Eisenberg & Price, *supra* note __, at § II.B.

[16] *Id.*

[17] *Id.* at I.D.

[18] Antonio Regalado, *23andMe Sells Data for Drug Search*, MIT TECH. REV. (June 21, 2016),

involved in care, and keep their data separate—potentially to be used for later commercial research. Non-care entities, like Fitbit (whose activity trackers monitor physical activity),[19] Apple (which aims to create a personal digital hub of health information),[20] or others, also generate health data—but they are, of course, largely separate from the system of health and hold different data in different places as well. Overall, different entities both within and outside the health care system generate data separately, which are then held in different siloes. This might not be so problematic if communication and data-sharing between the siloes were easy and seamless. Unfortunately, it isn't.

2. Data competition

Even for parallel entities, like multiple doctors that a patient may see, competition also keeps data fragmented. Theoretically, among care providers, competition should be irrelevant; the duty of care to patients should preclude competitive hoarding of data or refusal to share data. But no such pressure exists for the providers of diagnostic tests, for instance, or among others that collect health or health-related data.[21]

In addition to competition between those who generate data, there is competition between the vendors who provide ways of generating and managing data. The electronic health record market is itself fragmented, with hundreds of vendors.[22] This itself could lead organically to fragmentation

---

https://www.technologyreview.com/s/601506/23andme-sells-data-for-drug-search/ (describing 23andMe's collection of data and its sales of data subsets to over a dozen drug companies, including to Genentech for $10 million to search for Parkinson's drugs).

[19] Other sports companies are getting into the health data game. For instance, Nike recently signed a multimillion-dollar deal to collect and analyze performance data collected from athletes at the University of Michigan. Marc Tracy, *With Wearable Tech Deals, New Player Data Is Up for Grabs*, N.Y. TIMES (Sep. 9, 2016), http://www.nytimes.com/2016/09/11/sports/ncaafootball/wearable-technology-nike-privacy-college-football.html.

[20] *See* Apple, *iOS-Health*, http://www.apple.com/ios/health/ (describing the iOS Health App, which collects phone data and can serve as a repository for personal medical records).

[21] Perhaps the most well-documented such proprietary data silo is that held by Myriad Genetics, which amassed a dataset of information about women tested for mutations in the breast-cancer-related BRCA1 and BRCA2 genes while it held patents on those genes. *See*, *e.g.*, Misha Angrist & Robert Cook-Deegan, *Distributing the Future: The Weak Justifications for Keeping Human Genomic Databases Secret and the Challenges and Opportunities in Reverse Engineering Them*, 3 APPL. TRANSL. GENOMICS 124 (2014) (describing Myriad's dataset and others like it); Dan L. Burk, *Patents as Data Aggregators in Personalized Medicine*, 21 BU J. SCI. & TECH. L. 233 (2015) (describing how patents led to Myriad's competitive advantage).

[22] *See* OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, HOSPITAL HER VENDORS (July 2016), https://dashboard.healthit.gov/quickstats/pages/FIG-Vendors-of-EHRs-to-Participating-Hospitals.php. The top six vendors provide services for 92% of all nonfederal acute-care hospitals. *Id.*

through interoperability, as different vendors develop and sell different systems that might happen not to work with each other. However, there is evidence that electronic health record vendors do more, deliberately designing systems that are mutually incompatible to lock customers in and prevent easy migration between systems.[23] This lack of interoperability obviously hinders consolidation of data, transfers between providers as patients move, and the integration of care.

3. Legal barriers

A third barrier to integrating health data comes from legal barriers to data-sharing, especially the Health Insurance Portability and Accountability Act, commonly known as HIPAA.[24] HIPAA places limits on how personally identifiable health data may be used and disclosed.[25] In general, all uses and disclosures of such information by covered entities—providers, insurers, and health data clearinghouses[26]—are prohibited unless specifically permitted. To be sure, some permissions are quite broad, such as the use or disclosure of information for the purpose of "health care operations." Theoretically, this should make it easy to share information related to patient care. But HIPAA still creates substantial informal barriers; providers and insurers are notorious for refusing to share information with the blanket invocation of HIPAA, including for uses expressly permitted.[27]

HIPAA creates more substantial and formal barriers to sharing information for secondary research purposes. Research is expressly *not* a permitted purpose for use or disclosure of protected health information.[28] As

---

[23] *See* OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, REPORT TO CONGRESS: REPORT ON HEALTH INFORMATION BLOCKING 11–19 (April 2015), www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf (defining "information blocking" as "when persons or entities knowingly and unreasonably interfere with the exchange or use of electronic health information" and providing evidence of such practices).

[24] Pub. L. No. 104-191, 100 Stat. 2548.

[25] HIPAA's principal data restrictions come from the Privacy Rule, codified at 45 C.F.R. §§ 150ff. HIPAA's regulatory structure is complex and need not be discussed in full here; for additional information, *see*, *e.g.*, U.S. Dept. of Health and Human Services, *Summary of the HIPAA Privacy Rule* (May 2003), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/ (providing HIPAA overview); Eisenberg & Price, *supra* note 1, at __ (discussing the Privacy Rule in the context of research using existing health data).

[26] 45 C.F.R. § 160.103. Uses or disclosures by the business associates of covered entities are governed, though by contract rather than directly under HIPAA's Privacy Rule. 45 C.F.R. § 152(a)(3).

[27] For examples of refusals to share information, *see*, *e.g.*, Paula Span, *Hipaa's Use as Code of Silence Often Misinterprets the Law*, N.Y. TIMES (July 17, 2015), http:// www.nytimes.com/ 2015/07/21/health/hipaas-use-as-code-of-silence-often-misinterprets-the-law.html?_r=0.

[28] 21 C.F.R. § 164.501. Notably, an initial version of the 21st Century CURES Act included a provision adding research as a permissible purpose for use or, directing the

a result, secondary research often involves health information that has been de-identified, which takes it out of HIPAA's ambit.[29] However, as I have discussed elsewhere, de-identification can increase the fragmentation of health data, because reassembling data about a patient from different sources becomes substantially more difficult—deliberately so—without identifying information.[30] Finally, HIPAA creates barriers between different types of entities that assemble or create health data. HIPAA governs only "covered entities" that are directly involved in the health system. But increasingly, relevant health information is held by entities outside the that system, such as 23andMe, Fitbit, Apple, or others. None of these entities, or the data they hold, are directly governed by HIPAA.[31] Setting aside concerns this raises about fragmented *governance* of health data,[32] it also helps encourage fragmentation through disparate treatment of different entities with different forms of health data.

Notably, there have also been governmental efforts to encourage interoperability between different health data systems. The Office of the National Coordinator has set out a goal of electronic health record interoperability by 2021 to 2024.[33] And, of course, the push toward electronic health records was itself a federal initiative.[34] Other private systems have been created with the goal of collecting data across providers with the goal of ensuring continuous care and easing the processing of claims; however, these

---

Secretary of Health and Human Services to "revise or clarify" the Privacy Rule so that research "including studies whose purpose is to obtain generalizable knowledge" is included as part of the exception for health care operations. *See* H.R. 6 (2015), 114th Congress, § 1124, available at https://www.congress.gov/114/bills/hr6/BILLS-114hr6ih.xml). As passed, the legislation calls instead for the study of such an amendment to the Privacy Rule. Pub. L. No. 114-255 (2016), § 2063.

[29] HIPAA governs only personally identifiable health information; a safe harbor exempts any information from which 17 pieces of identifying information have been removed.

[30] *See* Price, *Patents, Big Data, and the Future of Medicine*, 37 CARDOZO L. REV. 1401, 1413 (2016).

[31] If these entities are business associates of covered entities, they may be regulatd by HIPAA as described in note 26, *supra*.

[32] *See* Nicolas Terry, *Regulatory Disruption and Arbitrage in Healthcare Data Protection*, 17 YALE J. HEALTH POL'Y, L., & ETHICS __ (2017).

[33] OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, CONNECTING HEALTH AND CARE FOR THE NATION: A 10-YEAR VISION TO ACHIEVE AN INTEROPERABLE HEALTH IT INFRASTRUCTURE (2014), http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf; OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, CONNECTING HEALTH AND CARE FOR THE NATION: A SHARED NATIONWIDE INTEROPERABILITY ROADMAP (Draft Version 1.0 April 2015), http://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf

[34] *See* ARRA, *supra* note 1.

efforts have met with real challenges.[35] Overall, health data in the US health care system remain highly fragmented among different entities, working with different and often mutually incompatible health records systems.

II. RISKS OF THE CURRENT SYSTEM

The risks from a fragmented health data system are substantial. These risks come in two main buckets: primary risks, which is to say risks to patients seeking care in the health system; and secondary risks, which is to say risks that arise when health data are repurposed and used to innovate or improve the system. The primary risks from a fragmented system of health data include, among others, problems in patient care and privacy risks to patient information.

The risks that arise in patient care mirror the potential benefits of electronic health records. If doctors are used to patient information being present in files—to indicate, for example, the presence of an allergy or a drug with potential negative interactions—doctors may be less likely to seek out or independently confirm that information in the absence of an EHR record. This works fine if the information is actually present, but decreases the likelihood of catch an error when the information is missing due to fragmentation or otherwise.

Similarly, to the extent that failures of interoperability and mistakes from assembling fragmented data introduce active errors in the system, this creates the chance for medical errors which can result in real harm to the patient. If, for instance, a medical administrator receives the records from a previous physician by fax and then adds them by hand to a patient's current record, he might accidentally introduce errors that can compromise future care.[36]

Lastly, when health data aren't meaningfully collected, we lose the opportunity to experience *better*, data-driven care than what we now receive. This isn't a classic "risk," but it does result in costs to patients measured in benefits foregone. To take a simple example, suppose that, as part of a

---

[35] For instance, a group of large insurers in California created Cal INDEX, a health information exchange with the goal of automatically collecting and linking patient data from many providers. *See* Cal INDEX, *New California Not-for-Profit to Operate Statewide, Next-Generation Health Information Exchange* (August 5, 2014), https://www.calindex.org/new-california-healthcare-exchange/ (last accessed July 16, 2016) ("Cal INDEX will securely collect and integrate clinical data from providers and claims data from payers to create comprehensive, retrievable patient-centered records known as longitudinal patient records (LPRs)"). The effort has met with limited success thus far. See Beth Kutcher, *Insurers build broad data exchange in California, but providers are slow to join*, MODERN HEALTHCARE (March 6, 2016), http://www.modernhealthcare.com/article/20160305/MAGAZINE/303059948.

[36] Sharona Hoffman & Andy Podgurski, *The Use and Misuse of Biomedical Data: Is Bigger Really Better?*, 39 AM. J. LAW MED. 497 (2013).

research study, a young woman has her genome sequenced;[37] further suppose that, although this woman not in a high-risk demographic group, she is in fact positive for an allele of the BRCA1 gene that substantially increases her risk of breast cancer. The researcher may not provide her with this information,[38] and there is a substantial likelihood that her genome sequence may be totally separate from her medical records used for primary care. Thus, the patient may not be more rigorously screened for breast cancer, as she would be if had been identified (by that doctor or another involved in her direct care) as a woman with a deleterious BRCA1 allele. In one sense, no new risk has been introduced—but in another, an opportunity for improved care has been missed.

The currently fragmented health data system also creates risks to patient privacy. Patient health data are considered by many to be especially sensitive, meaning that disclosure of such information is an especially substantial privacy concern.[39] Different actors in the system store information in different ways, leading both to less-secure implementations (in, for instance, the office of the solo practitioner that needs to duplicate and keep unnecessary information because it is not available from labs, insurers or specialists directly), and to potential vulnerabilities during information-sharing, when that occurs. Perhaps more importantly, the clunkiness of the system leads to workarounds and kludges that pose inherent security risks. For instance, problems with interoperability (and potentially with HIPAA) may be related to the otherwise-baffling persistence of faxed requests for information between different providers. Hand-answered, unvalidated, and difficult-to-audit fax requests suffer by comparison with high-security, auditable electronic data transfers, but remain the transfer mechanism of choice for some.[40]

---

[37] For the sake of the example, let us assume the lab is CLIA-certified, and that the genetic sequencing is thus of high-enough quality to guide clinical care.

[38] A substantial literature considers the question of returning results from genetic research. For an introduction, *see* Susan M. Wolf et al., *The Law of Incidental Findings in Human Subjects Research: Establishing Researchers' Duties*, 36 J. LAW. MED. ETHICS 361 (2008) (surveying the field); *see also* Ellen Wright Clayton & Amy L. McGuire, *The Legal Risks of Returning Results of Genomics Research*, 14 GENET. MED. 473 (2012) (noting legal risks); R. C. Green *et al.*, *ACMG Recommendations for Reporting of Incidental Findings in Clinical Exome and Genome Sequencing,"* 15 GENETICS MED. 565 (2013) (recommending that a set of identified mutations always be returned to patients); Paul S. Appelbaum et al., *Models of Consent to Return of Incidental Findings in Genomic Research*, 44 HASTINGS CTR. REP. 23 (2014) (noting different models of returning data and different possibilities for informed consent).

[39] *See* Roger A. Ford & W. Nicholson Price II*, Balancing Privacy and Accountability for Black-Box Medicine*, __ MICH. TELECOMM. & TECH. L. REV. __ (2017) (describing the privacy concerns related to patient health information); Nicolas Terry, *Protecting Patient Privacy in an Era of Big Data*, 81 UMKC L. REV. __ (2012).

[40] For instance, the University of Michigan Health System's request for records from another doctor—which itself must be filled out by the patient for each other provider, since

The secondary risks from fragmented data come from efforts to use those data for future innovation.[41] Such efforts include the FDA's Sentinel initiative to monitor drug usage for safety risks,[42] observational studies to drive care (which can potentially be used to approve new drug indications under the 21st Century Cures Act), machine-learning efforts to suss out new biological relationships,[43] and implementations of a learning health-care system generally.[44] All of these require that data be high-quality and function much better without substantial gaps in data from different sources or time periods. Fragmentation and errors in health data hinder these efforts. If they don't happen, that is one cost—the foregone benefit of innovation lost. But other risks materialize when innovation relies on incomplete or faulty data. To the extent that new care innovations are based on bad data, they may incorporate errors, biases, or other problems.[45] A fundamental datamining principle is "garbage in, garbage out;" when health care fragmentation creates inaccuracies in data later used in innovation, that innovation suffers, and so may future patients.

III. BENEFITS OF RESILIENT HEALTH DATA INFRASTRUCTURE

The risks of fragmented and insecure health data may be at least partially addressed by considering the system in terms of infrastructure—both *for* health data, and *of* health data.

First, the continued fragmentation of health data suggests that the current system is unsustainable. Each actor is responsible for generating, collecting, and storing the data for its own interactions with patients in the health system, and this has led to the substantial risks described above. Given the potential benefits of integrated patient data, effort must be expended at a systemic level to create infrastructure for the sharing, integration, and storage of patient data. This effort need not take any specific form, but the idea of infrastructure for health data, and the risks of fragmented health data, suggest some features of the desired state.

An infrastructure for health data could follow different models of varying centralization. It could exist as a centralized health database, where each

---

no centralized system exists) offers options only for phoning or faxing to request records from another provider.

[41] *See generally* Eisenberg & Price, *supra* note 1 (describing potential innovation by health-care payers using existing health data).

[42] Susan Forrow et al., *The Organizational Structure and Governing Principles of the Food and Drug Administration's Mini-Sentinel Pilot Program*, 21 PHARMACOEPIDEMIOL. DRUG SAF. 12 (2012).

[43] *See* Price, *Black-Box Medicine*, *supra* note __.

[44] *See*, *e.g.*, Harlan M. Krumholz, *Big Data and New Knowledge in Medicine: The Thinking, Training, and Tools Needed for a Learning Health System*, 33 HEALTH AFF. 1163 (2014).

[45] *See*, *e.g.*, Sharona Hoffman & Andy Podgurski, *Big Bad Data: Law, Public Health, and Biomedical Databases*, 41 J.L. MED. ETHICS 56 (2013).

patient has a single integrated patient record to which different care providers or other entities add data. Alternately, health data could reside in decentralized repositories, much like the current system, but with increased connectivity between the repositories and more rigorous standards that let data be meaningfully transferred between and collated across repositories. This model is closest to the current system—but that closeness demonstrates potential problems, since even with federal initiatives to drive interoperability, fragmentation persists.[46] A fully decentralized system might have individual patients maintain their own data, such as on a personal medical card that includes the entire patient record. Such a system would similarly rely on meaningful standards to ensure transportability and access of patient data by different actors in the health care system.

Any of these systems might potentially work as infrastructure *for* health data, to help enable care. However, a centralized system carries a substantial benefit when considering health data *as* infrastructure for later health innovation. Decentralized data are fragmented along different dimension—not necessarily among different providers and actors in the health system, but between different patients. However, many benefits of health data rely on aggregating data from many patients, including precision medicine, quality metrics, and efficiency measures. The risks for health innovation described above include the problems of biases from incomplete data and the risk of innovation being absent altogether. Centralized health data ameliorate these risks by creating comprehensive datasets for future analysis.

Centralized infrastructure goods are typically undersupplied because they are classic public goods; that is, they are nonexcludable and nonrivalrous.[47] Accordingly, we expect private actors to invest at suboptimal levels in infrastructure spending, suggesting a need for some form of central investment. The federal government is an obvious choice, and indeed the federal government already operates substantial examples of health data infrastructure.[48] These include the multi-site-but-connected Sentinel Project (wherein FDA collects safety information on drugs in use),[49] the Medicare and Medicaid systems, the Veterans Administration,[50] and—specifically focused on forward-looking health research—the Precision Medicine Initiative, aiming to

---

[46] *See supra* Section I.B.

[47] For an extensive theory of infrastructure, *see* BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES (2013).

[48] *See* Eisenberg & Price, *supra* note 1, at __.

[49] See Health Affairs, *Health Affairs Health Policy Brief, The FDA's Sentinel Initiative*. (June 4, 2015), http://healthaffairs.org/healthpolicybriefs/brief_pdfs/healthpolicybrief_139.pdf; Price, *Big Data, Patents, and the Future of Medicine*, *supra* note 30, at __ (describing the Sentinel project's data implications).

[50] *See* Price, *Big Data, Patents, and the Future of Medicine*, *supra* note 30, at __ (describing the Veterans Administration's data).

collect comprehensive data on at least one million Americans.[51] An alternate model could rely on public-private partnerships, joining a central government authority with nonprofit actors. However, there is no fundamental requirement that the infrastructure provider be governmental or nonprofit; a for-profit entity can provide public infrastructure given appropriate incentives.[52]

Centralization has complex effects on potential privacy risks. On the one hand, centralization creates a broader picture of an individual's health—indeed, that's the point—but that makes it easier to derive more information about an already-identified individual, and also potentially makes it easier to identify a de-identified individual from a larger collection of data.[53] A centralized system is also a more attractive target for attacks. On the other hand, centralization, or just a coherent infrastructure, allows some privacy-enhancing technologies to be deployed, such as one-way hashing, dataset-docking, or simply scaled security given the possible concentration of resources at a single location.

CONCLUSION

The health system relies on data, but collects and maintains those data in a haphazard, fragmented, and insecure way that creates real risks for patients and for the system as a whole. Given market incentives driving competition among different data systems and health actors, health data seem likely to remain fragmented without broader systemic action. Conceiving of infrastructure both for and of health data suggests that standardized, centralized collection and maintenance of health data may create goods at both the individual and systemic level. If we are to realize the goal of data-informed patient care and data-driven development of future medical technology, an infrastructure for health data provides a substantial step in the right direction.

---

[51] *Id.* at __; Francis S. Collins & Harold Varmus, *A New Initiative on Precision Medicine*, 372 N. ENGL. J. MED. 793 (2015).

[52] Examples include toll-road operators, power companies, and other public utilities. Of course, these monopolies raise their own concerns about potential rent-seeking behavior.

[53] For instance, there may be many people in a particular health system that fit two or three given characteristics; many fewer fit twenty or thirty, and two or three hundred would be much more likely to apply only to a single individual. *Cf.* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

Mitigating the Increasing Risks of an Insecure Internet of Things

Nick Feamster
Princeton University

1 Introduction

The emergence and proliferation of Internet of Things (IoT) devices on industrial, enterprise, and home networks brings with it unprecedented risk. The potential magnitude of this risk was made concrete in October 2016, when insecure Internet-connected cameras launched a distributed denial of service (DDoS) attack on Dyn, a provider of DNS service for many large online service providers (e.g., Twitter, Reddit) [5, 8]. Although this incident caused large-scale disruption, it is noteworthy that the attack involved only a few hundred thousand endpoints and a traffic rate of about 1.2 terabits per second. With predictions of upwards of a billion IoT devices within the next five to ten years [6], the risk of similar, yet much larger attacks, is imminent.

2 The Growing Risks of Insecure IoT Devices

One of the biggest contributors to the risk of future attack is the fact that many IoT devices have long-standing, widely known software vulnerabilities that make them vulnerable to exploit and control by remote attackers. Worse yet, the vendors of these IoT devices often have provenance in the hardware industry, but they may lack expertise or resources in software development and systems security. As a result, IoT device manufacturers may ship devices that are extremely difficult, if not practically impossible, to secure [4, 9]. The large number of insecure IoT devices connected to the Internet poses unprecedented risks to consumer privacy, as well as threats to the underlying physical infrastructure and the global Internet at large:

- **Data privacy risks.** Internet-connected devices increasingly collect data about the physical world, including information about the functioning of infrastructure such as the power grid and transportation systems, as well as personal or private data on individual consumers. At present, many IoT devices either do not encrypt their communications or use a form of encrypted transport that is vulnerable to attack [3]. Many of these devices also store the data they collect in cloud-hosted services, which may be the target of data breaches or other attack [1].
- **Risks to availability of critical infrastructure and the Internet at large.** As the Mirai botnet attack of October 2016 demonstrated, Internet services often share underlying dependencies on the underlying infrastructure: crippling many websites offline did not require direct attacks on these services, but rather a targeted attack on the underlying infrastructure on which many of these services depend (i.e., the Domain Name System). More broadly, one might expect future attacks that target not just the Internet infrastructure but also physical infrastructure that is increasingly Internet- connected (e.g., power and water systems). The dependencies that are inherent in the current Internet architecture create immediate threats to resilience.

The large magnitude and broad scope of these risks implore us to seek solutions that will improve infrastructure resilience in the face of Internet-connected devices that are extremely difficult to secure. A central question in this problem area concerns the responsibility that each stakeholder in this ecosystem should bear, and the respective roles of technology and regulation (whether via industry self-regulation or otherwise) in securing both the Internet and associated physical infrastructure against these increased risks.

3 Risk Mitigation and Management

One possible lever for either government or self-regulation is the IoT device *manufacturers*. One possibility, for example, might be a device certification program for manufacturers that could attest to adherence to best common practice for device and software security. A well-known (and oft-used) analogy is the UL certification process for electrical devices and appliances.

Despite its conceptual appeal, however, a certification approach poses several practical challenges. One challenge is outlining and prescribing best common practices in the first place, particularly due to the rate at which technology (and attacks) progress. Any specific set of prescriptions runs the risk of falling out of date as technology advances; similarly, certification can readily devolve into a checklist of attributes that vendors satisfy, without necessarily adhering to the process by which these devices are secured over time. As daunting as challenges of specifying a certification program may seem, enforcing adherence to a certification program may prove even more challenging. Specifically, consumers may not appreciate the value of certification, particularly if meeting the requirements of certification increases the cost of a device. This concern may be particularly acute for consumer IoT,

where consumers may not bear the direct costs of connecting insecure devices to their home networks.

The *consumer* is another stakeholder who could be incentivized to improve the security of the devices that they connect to their networks (in addition to more effectively securing the networks to which they connect these devices). As the entity who purchases and ultimately connects IoT devices to the network, the consumer appears well-situated to ensure the security of the IoT devices on their respective networks. Unfortunately, the picture is a bit more nuanced. First, consumers typically lack either the aptitude or interest (or both!) to secure either their own networks or the devices that they connect to them. Home broadband Internet access users have generally proved to be poor at applying software updates in a timely fashion [7], for example, and have been equally delinquent in securing their home networks [2]. Even skilled network administrators regularly face network misconfigurations, attacks, and data breaches. Second, in many cases, users may lack the incentives to ensure that their devices are secure. In the case of the Mirai botnet, for example, consumers did not directly face the brunt of the attack; rather, the ultimate victims of the attack were DNS service providers and, indirectly, online service providers such as Twitter. To the first order, consumers suffered little direct consequence as a result of insecure devices on their networks.

Consumers' misaligned incentives suggest several possible courses of action. One approach might involve placing some responsibility or liability on consumers for the devices that they connect to the network, in the same way that a citizen might be fined for other transgressions that have externalities (e.g., fines for noise or environmental pollution). Alternatively, Internet service providers (or another entity) might offer users a credit for purchasing and connecting only devices that it pass certification; another variation of this approach might require users to purchase "Internet insurance" from their Internet service providers that could help offset the cost of future attacks. Consumers might receive credits or lower premiums based on the risk associated with their behavior (i.e., their software update practices, results from security audits of devices that they connect to the network).

A third stakeholder to consider is the *Internet service provider (ISP)*, who provides Internet connectivity to the consumer. The ISP has considerable incentives to ensure that the devices that its customer connects to the network are secure: insecure devices increase the presence of attack traffic and may ultimately degrade Internet service or performance for the rest of the ISPs' customers. From a technical perspective, the ISP is also in a uniquely effective position to detect and squelch attack traffic coming from IoT devices. Yet, relying on the ISP alone to protect the network against insecure IoT devices is fraught with non-technical complications. Specifically, while the ISP could technically defend against an attack by disconnecting or firewalling consumer devices that are launching attacks, such an approach will certainly result in increased complaints and technical support calls from customers, who connect devices to the network and simply expect them to work. Second, many of the technical capabilities that an ISP might have at its disposal (e.g., the ability to identify attack traffic coming from a specific device) introduce serious privacy concerns. For example, being able to alert a customer to (say) a compromised baby monitor requires the ISP to know (and document) that a consumer has such a device in the first place.

Ultimately, managing the increased risks associated with insecure IoT devices may require action from all three stakeholders. Some of the salient questions will concern how the risks can be best balanced against the higher operational costs that will be associated with improving security, as well as who will ultimately bear these responsibilities and costs.

4 Improving Infrastructure Resilience

In addition to improving defenses against the insecure devices themselves, it is also critical to determine how to better build resilience into the underlying Internet infrastructure to cope with these attacks. If one views the occasional IoT-based attack inevitable to some degree, one major concern is ensuring that the Internet Infrastructure (and the associated cyberphysical infrastructure) remains both secure and available in the face of attack. In the case of the Mirai attack on Dyn, for example, the severity of the attack was exacerbated by the fact that many online services depended on the infrastructure that was attacked. Computer scientists and Internet engineers should be thinking about technologies that can both potentially decouple these underlying dependencies and ensure that the infrastructure itself remains secure even in the event that regulatory or legal levers fail to prevent every attack. One possibility that we are exploring, for example, is the role that an automated home network firewall could play in (1) helping users keep better inventory of connected IoT devices; (2) providing users both visibility into and control over the traffic flows that these devices send.

5 Summary

Improving the resilience of the Internet and cyberphysical infrastructure in the face of insecure IoT devices will require a combination of technical and regulatory mechanisms. Engineers and regulators will need to work together to improve security and privacy of the Internet of Things. Engineers must continue to advance the state of the art in technologies ranging from lightweight encryption to statistical network anomaly detection to help reduce risk; similarly, engineers must design the network to improve resilience in the face of the increased risk of attack. On the other hand, realizing these advances in deployment will require the appropriate alignment of incentives, so that the parties that introduce risks are more aligned with those who bear the costs of the resulting attacks.

References

[1] Asus settles ftc charges that insecure home routers and cloud services put consumers privacy at risk, Feb. (Cited on page 1.)

[2] R. Grinter et al. The Work to Make a Home Network Work. In *ECSCW*, 2005. http://www.cc.gatech.edu/~beki/c27.pdf. (Cited on page 2.)

[3] S. Grover and N. Feamster. The Internet of Unpatched Things. In *PrivacyCon*, Washington, DC, Jan. 2016. Federal Trade Commission. https://www.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf. (Cited on page 1.)

[4] B. Krebs. IoT Reality: Smart devices, Dumb defaults, Feb. 2016. http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/. (Cited on page 1.)

[5] B. Krebs. KrebsOnSecurity Hit with Record DDoS, Oct. 2016. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. (Cited on page 1.)

[6] J. Manika et al. The internet of things: Mapping the value beyond the hype. Technical report, McKinsey Global Institute, June 2015. (Cited on page 1.)

[7] A. Mathur et al. They Keep Coming Back Like Zombies: Improving Software Updating Interfaces. In *USENIX Symposium on Usable Security and Privacy*, 2016. https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-mathur.pdf. (Cited on page 2.)

[8] N. Perlroth. Hackers Used New Weapons to Disrupt Major Websites Across U.S., Oct. 2016. https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html. (Cited on page 1.)

[9] B. Schneier. The internet of things is wildly insecure and often unpatchable, Jan. 2014. https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html. (Cited on page 1.)