The New Frontiers of Privacy Harm
A report on a Silicon Flatirons Conference
University of Colorado Law School
January 17, 2014

By: Laura Littman, Mindy Swaney, and Amber Williams

A video of the conference and the conference agenda are available at http://www.silicon-flatirons.org/events.php?id=1381.

Panel 1: Is Government Surveillance Harmful?

Panel: Susan Freiwald, Professor, University of San Francisco School of Law; Todd Hinnen, Partner, Perkins Coie; Ashkan Soltani, Independent Researcher and Consultant, Soltani LLC; Omer Tene, Vice Presient of Research and Education, IAPP; Vice Dean, College of Management School of Law, Rishon Le Zion, Israel; Ben Wizner, Director, American Civil Liberties Union Speech, Privacy & Technology Project. Moderator: Paul Ohm, Associate Professor of Law, University of Colorado; IP/IT Initiative Director, Silicon Flatirons Center.

The conference began with an impromptu live streaming of President Obama's speech on NSA reforms.[1] Following the President's speech, the first panel responded to questions asked by Paul Ohm about the speech. Next, the panel discussed the harm associated with government surveillance.

NSA: First, the panelists discussed the effects of NSA surveillance and the Snowden leaks. In response to President Obama's proposed new judicial oversights, the panel pointed out that the judicial oversights will be significant because the NSA poses statutory and constitutional legal questions. Next, the panelists discussed the evolution of the NSA and how America got to this point. The public tolerates the NSA's operations because people believe that the NSA protects America against terrorist attacks. However, one panelist said that so far, the NSA's surveillance has only caught on person who sent $8,000 to al-Shabob in Somalia. There was consensus that the NSA is extremely powerful because they possess and collect mass information. Finally, the panelists pointed out that the NSA could infer that every one of us is involved in a crime at some point by using this system of analyzing mass information.

Mass Monitoring and Surveillance: Next, the panelists discussed the harms of mass monitoring and surveillance. The panelists questioned the justifications of these practices and whether a computer could wholly automate the practices or whether the monitoring should have elements of human intervention. The panelists highlighted the fact that no one knows if mass surveillance and monitoring actually works and protects anyone. However, there were sentiments that they

[1] Transcript of President Obama's Jan. 17 speech on NSA reforms, Washington Post (January 17, 2014), http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

hoped it worked. The panelists pointed out a purpose for the Fourth Amendment, which is preventing a government to gain too much power. Thus, keeping in mind this understanding of the Fourth Amendment, the panelists discussed NSA surveillance and other forms of surveillance used regularly. The panelists discussed how real time surveillance, such as current location and current video monitoring, are (or at least feel) more intrusive than stored data that is then analyzed. All of the panelists expressed that they believe every person in America could be subject to government monitoring under current practices.

Panel 2: Is Commercial Tracking Harmful?

Panel: Julia Angwin, Journalist and Author; James C. Cooper, Director, Research and Policy, Law and Economics Center, School of Law, George Mason University; Edward Felten, Director, Center for Information Technology Policy; Professor of Computer Science and Public Affairs, Princeton University; Fran Maier, Founder and Chair of the Board, TRUSTe. Moderator: Scott Peppet, Professor of Law, University of Colorado.

The second panel discussed the harms of commercial tracking and the risks that are associated with collecting consumer data.

Commercial manipulation: Julia Angwin began the discussion by presenting her new book, Dragnet Nation. The book has a theme, which is that information is power. This power, she said, can be good and bad—but there is no doubt that it is powerful. For example, the data collection practices that commercial entities engage in that create targeted ads that pop up on our computers and other devices shape the choices we make. The panelists discussed what this power means on a mass scale and warned that it provides a way for the advertising industry to potentially harmfully manipulate people. The panelists pointed out how commercial trackers, such as cookies, can be used in ways to manipulate people. Additionally, people can be found via their phones or other GPS trackers and watched on cameras (for example, hackers have taken over webcams to take pictures of naked women and use those pictures to extort money), Google glasses, and drones. There is also the risk of identity theft, and some of the panelists were surprised about the Google algorithm during the past presidential election that inserted Obama or Romney into search results after someone previously searched for either of the candidates.

Chilling effect of commercial tracking: The panelists agreed that there is a chilling effect when one thinks about being watched. The panelists discussed how people feel harm differently. One person may not care that Google Chrome is tracking your every online move, but others, such as some of the panelists, want to be private and do not like the idea of their information being sold to data miners. There is a public choice in the matter that drives legislation because privacy has a subjective measure of harm. Moreover, privacy's subjective nature makes it difficult to measure accurately. The panelists pointed out that the harm caused by hacked consumer information is large in scope and consumers are not capable of retaliation or protection against the people who hack their personal information.

Consumer Choice: The panelists discussed the decreasing opportunity for consumers to choose what they want to do or buy online because ads are specifically targeted to them. One example is that someone of higher income will be shown a more expensive car on an automobile website than a lower income individual on the same website. The panelists also discussed the effects of price discrimination. For example, certain Staples stores charge more if they are located near an affluent neighborhood and might charge less if they are competing against an OfficeMax or other office supply superstore. This process of price discrimination is a form of redlining, but the panelists are not sure what the future of redlining will be. The panelists discussed statistics, including that 86 percent of consumers know that they are tracked on the internet, 70 percent of consumers know their phones are being tracked, 90 percent of consumers are taking action to protect themselves, and only 17 percent of consumers would pay more money to avoid ads.

Consent: Importantly, many panelists believe that most consumers do not actually know what they are consenting to a majority of the time. Today, we know more about what data is being collected, but the panelists agreed that it is very difficult to protect one's privacy completely. For example, one panelist highlighted that it is very difficult to fix one's credit report after his or her identity has been stolen. Another panelist said that notwithstanding her efforts in contracting over 200 data companies to have her information removed form the internet, a friend still found her address online.

Keynote Address: Julie Brill, *Commissioner*, Federal Trade Commission

Commissioner Brill has dedicated her career to protecting consumers. With her extensive knowledge about consumer protection issues and her diverse experience working in several state attorney generals' antitrust and consumer protection divisions, Commissioner Brill provides a distinctive perspective on how government agencies conceptualize harm.

In her remarks, Commissioner Brill focused on how the FTC identifies both concrete and abstract harms. Concrete harms are more easily identified, such as financial harm stemming from identity theft. Abstract harms are harder to ascertain. For example, the breach of protected health information is harmful to the consumer because of the highly personal and sensitive nature of the information being revealed. Commissioner Brill noted that the line between concrete and abstract harms is blurring and that the FTC's consideration of concrete and abstract harms has evolved over the decades. However, she noted that the agency is limited to what can be brought under the Federal Trade Commission's Act.

Commissioner Brill discussed a recent FTC case brought for non-monetary harm involving rent-to-own companies installing software on rental laptops to spy on consumers. Additionally, she discussed other cases involving unfair practices, including a charge against Facebook for engaging in material retroactive changes to their privacy policies; a case against the social networking app Path, which collected consumers' contact information without notification to the users; and a case concerning P2P software taking data from consumers and sharing it without

their knowledge. Commissioner Brill stated that these are the kinds of cases that represent non-monetary harm.

Next, Commissioner Brill briefly discussed the effects of Edward Snowden on commercial privacy and data security, which she thinks has heightened our sense of awareness about big data.

On another note, when asked about the FTC's "soft law" enforcement (the release of reports, workshops, consent decrees, and studies) Commissioner Brill stated that the FTC views these products as giving guidance to companies, much like the common law. Further, she noted that companies actively seek out the FTC's opinion on matters.

Next, Commission Brill stated that she worries about the extensive big data profiles being created on consumers because they may contain sensitive health information. Additionally, she is concerned that it is getting increasingly harder for consumers to identify when a device or app is collecting data.

On the topic of data security and the recent breach of credit card information at Target, Commission Brill said that data breaches are a serious concern because they affect consumers in a multitude of ways and the ramifications last for several years. When asked if companies should be given safe harbors for data breaches, Commissioner Brill said that the FTC is only concerned with examining a company's security practices and procedures to see if they are reasonable and not all breaches result in action. She said it is time for the United States to become "a first world country" regarding the use of credit cards.

Panel 3: Measuring Harm and the Risk of Harm
Panel: Ryan Calo, Assistant Professor of Law, University of Washington; Deven McGraw, Director of the Health Privacy Project, Center for Democracy and Technology; Adam Thierer, Senior Research Fellow, Mercatus Center, George Mason University; Christopher Wolf, Partner, Hogan Lovells; David Zetoony, Partner, Bryan Cave LLP.
Moderator: Meg Ambrose, Assistant Professor, Communication, Culture, and Technology (CCT), Georgetown University.

The third panel of experts discussed how to assess risk and measure privacy harm.

Assessing Risk:

Presenter Ryan Calo opened the panel by discussing how to assess privacy risk. Mr. Calo stated that he conceptualizes privacy harm by thinking about the key players and their capabilities, incentives, and motivations. He identified three situations where privacy harm occurs: peer-to-peer harm, harm to citizens by the government, and harm to consumers by corporations. Mr. Calo believes that law and policy should be cognizant of who has the capacity to do the most harm and that the assessment of risk involves determining future behavior.

Presenter Deven McGraw discussed the assessment of risk in relation to health data. The breach of private health information results in lost trust between the consumer and health care provider. Survey data reveals that consumers practice privacy protection behaviors in reaction to their lack of confidence in the health care industry. These behaviors include avoiding care or choosing to withhold specific health information. Additionally, Ms. McGraw discussed how HIPAA regulates health data risk. HIPAA allows for the routine use of data without consent from the data subject and requires business associates to execute agreements on the use and disclosure of private health information. Ms. McGraw said that the current health privacy regulations are not risk-based and need to be revised to adequately address consumers' concerns about privacy.

Presenter Christopher Wolf talked about how businesses assess privacy risks. He believes that businesses understand that when they develop products and services, they should follow the mantra "do no harm." Assessing privacy harm involves awareness about existing laws, regulations, and anticipating future enforcement actions. Mr. Wolf stated that the law is merely a starting point when assessing privacy harm. He thinks the focus on notice, consent, and collection inevitably misses fundamental privacy harms and is under inclusive. The law does not sufficiently address intangible harms like reputational and social stigma. When businesses inventory privacy harms by identifying vulnerable groups or the retention of large data sets, they are better equipped to manage risk.

Measuring Harm:

Discussant Adam Thierer stated that the further we move away from the ideology that privacy is tied to some unambiguous thing (i.e. the self, home, etc.) the harder it will be to classify and measure harm. Secondly, the accelerated pace that norms and standards are changing makes it difficult to measure harm. Mr. Theirer discussed why privacy information controls are costly and identified alternative remedies, including media literacy and digital ethics.

Finally, Discussant David Zetoony highlighted how businesses measure harm. Most companies are not market makers (e.g. innovators) but market takers. When market takers measure harm, they try to quantify the harm. One way to quantify the harm is to measure financial risk, including fines and penalties by regulatory agencies.

During the question and answer portion of the panel, the panelists generally agreed that if the harm cannot be measured, the harm cannot be governed. Additionally, the panelists brought up the Target data breach and the pregnancy coupon issue as examples of harm. Mr. Wolf highlighted that companies are now bringing in consultants to address privacy concerns and potential harm.

Panel 4: Tailoring Solutions to Privacy Harm Through Regulation, Architecture, and Self-Regulation

Panel: Alvaro Bedoya, Chief Counsel, Senate Judiciary Subcommittee on Privacy, Technology and the Law, United States Senate; Paula Bruening, Senior Counsel, Global Privacy Policy, Intel; Woodrow Hartzog, Assistant Professor, Cumberland School of Law, Stamford University; Michael Hintze, Chief Privacy Counsel and Assistant General Counsel, Microsoft Corporation; Rob Sherman, Manager of Privacy and Public Policy, Facebook. Moderator: Harry Surden, Associate Professor of Law, University of Colorado.

The last panel discussed how to manage and reduce privacy harms.

Privacy protections and solutions: Presenter Mr. Hartzog stated that it is harder to tailor solutions when the harm is indirect and opaque. Mr. Hartzog believes that modest privacy protections are undervalued and might be the best way to address indirect and opaque harms. Modest protections include limiting protection of private information to a short period of time or requiring design controls involving notice and consent. He stated that modest solutions can apply to a much broader class of harms and are politically palpable.

Effectiveness of limited and modest privacy protections: In response to Mr. Hartzog's presentation, the panel discussed whether limited or modest protections are sufficient to address privacy harms. Mr. Sherman stated that the regime is more flexible and people have been empowered to take control of their privacy. Mr. Hintze commented that he disagrees with Mr. Hartzog's argument that piecemeal state privacy legislation is an effective solution. Mr. Hintze stated it would be more helpful to have a single baseline standard for companies to follow. Ms. Bruening framed the use of modest protections as one of many tools to solve privacy harm.

Government intervention as a solution for privacy harm: Mr. Bedoya talked about two harmful activities: GPS stocking and NSA tracking. Mr. Hintze commented that an absolute prohibition on specific technology is more likely to lead to unintended consequences. However, he thinks that increased disclosure by businesses is necessary to address privacy harm. The panel agreed that absolute prohibitions are just one tool in the solution toolbox.

Private sector self-regulation: The panel supported self-regulation but stated a preference for baseline regulations. Mr. Sherman stated that consumers need to have confidence in a company's treatment of private information and, although it is hard to measure "creepy," a company can take active steps to measure harm. Ms. Bruening added that co-regulation seems to be a more operable and effective solution.

Privacy by design: To close, the panel discussed privacy by design as a solution. Mr. Sherman and Mr. Hintze explained that Microsoft and Facebook are taking active steps to design services and products with privacy as a focal point.