Maryland Law Review

Volume 76 | Issue 4 Article 3

Privacy, Security, and the Connected Hairbrush

Travis LeBlanc

Symposium Essays from *The State of Cyberlaw: Security and Privacy in the Digital Age*

Hosted by the *Maryland Law Review* at the
University of Maryland Francis King Carey School of Law
February 10, 2017

PRIVACY, SECURITY, AND THE CONNECTED HAIRBRUSH

TRAVIS LEBLANC*

REMARKS ADAPTED FROM KEYNOTE ADDRESS

Good afternoon, and thank you to Joshua Carback, Hannah Cole-Chu, and everyone at the University of Maryland Francis King Carey School of Law and the *Maryland Law Review* for putting this excellent event together and graciously inviting me to participate. I am truly honored to address you today in the presence of so many of the nation's leading privacy and security scholars, advocates, and practitioners.

The law school and the *Law Review* really are to be commended for putting together such a talented and distinguished lineup of privacy all-stars. The panelists that you heard from this morning and the ones that you will hear from this afternoon are leaders in the field. They tirelessly work every day, crisscrossing the country and the globe, to advance the public dialogue on privacy and security issues.

As Josh mentioned, until recently, I served as Chief of the Enforcement Bureau at the Federal Communications Commission ("FCC"). Prior to that, I served as Special Assistant Attorney General of California and senior advisor to then Attorney General, now Senator, Kamala D. Harris. In both of these positions, I had the opportunity to serve at the forefront of privacy and cyber security policy, regulation, and enforcement.

During my time in California, I spearheaded initiatives to bring more transparency to consumers about mobile privacy practices, including requirements for commercial websites and mobile app developers to post publicly

* Partner, Boies Schiller Flexner LLP; former Enforcement Bureau Chief, Federal Communications Commission (2014–2017).

available privacy policies. We take mobile privacy policies for granted today. Indeed, privacy researchers have extensively documented how few consumers actually read privacy policies. And they are right about the general lack of consumer review, particularly given the sheer number of online services that we all use, the length of these policies, the legalese in which they are drafted, and the overall tendency of many privacy policies to emphasize everything that a company may collect or do without clearly and conspicuously disclosing what they actually do.

Despite these drawbacks, however, I remain an advocate for formal privacy policies.[1] I also believe these policies should be complimented by consumer-friendly disclosures, such as just-in-time notifications.[2] You see, privacy policies have become fertile territory for advocates, academics, and government enforcers. These policies also have the significant benefit of employing thousands of privacy professionals around the world! There was a time not that long ago, however, when privacy policies were largely absent in the mobile space.[3] That was unacceptable in California and we worked to use California's one-of-a-kind Online Privacy Protection Act[4] as a tool to promote transparency in mobile privacy.

While in California, I also worked in the Attorney General's Office to establish a Privacy Enforcement and Protection Unit and to implement initiatives to provide additional guidance to mobile app developers, ad networks, carriers, and others on how to approach privacy in this ever-changing mobile environment.[5] I took these same principles with me when I moved to the FCC. As Chief of the Enforcement Bureau, I established and led a team focused on the privacy and security issues that matter most to consumers—privacy and security of their personal information ranking high among them. Under my leadership, the Bureau worked to enforce the duty that all telecommunications, cable, satellite, and broadband Internet companies have to protect consumers' personal information. In three years, we imposed $50 million in fines related to privacy and security.[6]

---

1. *See generally* Mike Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044 (2017) (arguing that detailed privacy statements provide greater transparency and accountability with respect to an organization's data collection practices).

2. *See also* KAMALA D. HARRIS, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.

3. *See, e.g.*, Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J. (Dec. 17, 2010), https://www.wsj.com/articles/SB10001424052748704694004576020083703574602.

4. CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2008).

5. *See, e.g.*, HARRIS, *supra* note 2.

6. Press Release, Fed. Commc'n Comm'n, FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-In for Third Parties (Mar. 7, 2016), https://www.fcc.gov/document/fcc-settles-verizon-supercookie-probe; Press Release, Fed. Commc'n Comm'n, Cox Communications to

But, today, I do not want to focus my remarks on the privacy and security concerns with the network. Rather, I want to talk with you today about the how these concerns are unraveling with the billions of devices that are connected to the world's largest network, namely, the Internet.

As you all know, today, more devices than ever are connected to the Internet. Everything from your smartphone to your toaster and even your toothbrush and hairbrush now are able to be connected to the Internet. Actually, let me pause here for one moment: Seriously, do we really need to have a hairbrush connected to the Internet? Let me assure you it exists. I had the opportunity to see it at the Consumer Electronics Show ("CES") in January.[7] The hairbrush contains sensors and a microphone that records the sound of breaking hair and vibrates to alert you if you brush your hair too hard. And then, at the end of your hairbrushing session, it gives you a rating of your hair's health, of course taking into account humidity, temperature, and wind. The craziest part about my experience with this "smart" hairbrush is that when my colleague looked at the brush's mobile app to see what it said about her session, the app conveyed an inspiring message: "YOUR HAIR IS UNRULY."

This growing interconnectedness of everything has been called the "Internet of Things," the "Internet of Everything," and even the "Fourth Industrial Revolution." But, to be clear, the Internet of Things ("IOT") is not something to be talked about and dealt with in the future. It is already here and it is only growing! It is predicted that by 2020 there will be 50 billion devices connected to the Internet—that's billion with a "b."[8]

To put in perspective how explosive this growth has been in a short period:

- Fourteen years ago, there were an estimated 500 million connected devices;

Pay $595,000 to Settle Data Breach Investigation (Nov. 5, 2015), https://www.fcc.gov/document/cox-communications-pay-595000-settle-data-breach-investigation-0; Press Release, Fed. Commc'n Comm'n, AT&T to Pay $25 Million to Settle Consumer Privacy Investigation (Apr. 8, 2015), https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0; Press Release, Fed. Commc'n Comm'n, Verizon to Pay $7.4 Million to Settle Consumer Privacy Investigation (Sept. 3, 2014), https://www.fcc.gov/document/verizon-pay-74m-settle-privacy-investigation-0.

7. Brian Heater, *Here's a Smart Hairbrush with a Built-in Microphone from Withings and L'Oreal*, TECHCRUNCH (Jan. 3, 2017), https://techcrunch.com/2017/01/03/withings-brush/; Brett Molina, *CES 2017: Why Do We Even Need a Wi-Fi Hairbrush?*, USA TODAY (Jan. 5, 2017, 3:16 PM), https://www.usatoday.com/story/tech/talkingtech/2017/01/05/ces-2017-even-your-hairbrush-can-connect-wi-fi/96196376/.

8. DAVE EVANS, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING (2011), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

- In just seven years, by 2010, that number exploded to 12.5 billion; *and*
- In ten more years, by 2020, that number is expected to quadruple to 50 billion.[9]

Keep in mind, there are around 7.5 billion people on the planet, so by 2020 that could be about seven connected devices per person. However, considering that some reports have estimated that more than half of the global population still does not have regular access to the Internet,[10] there could be upwards of sixteen devices per person in areas that are fortunate enough to have regular Internet access. These billions of devices will have the potential to access, transmit, and analyze petabytes of data in real time. For those who don't know what a petabyte is, it is approximately 1024 terabytes, or a million gigabytes. That is a lot of shared data!

This is all extremely exciting, but it also presents many challenges. The security of these devices, and the massive amounts of information they generate, are crucial to the success of this digital revolution. The world is anxious to adopt these devices, but that confidence will be shaken if industry and the government don't get privacy and security right. We need to find the right balance to ensure these billions of devices are secure and that consumer data is not only protected, but that the collection and use of that data also meet consumer expectations. Considering the variety of items that now can connect to the network, including things like children's toys, consumers need to have the ability to know and decide what information they are comfortable sharing and be provided opportunities to control the sharing of that information.

There is no denying the massive benefits that these connected devices can provide. To fully understand and appreciate the benefits, you need to understand the vastness of connected devices now available. Obviously this includes smart phones, tablets, and over-the-top video products like Apple TV or Google TV. But it also includes connected health products—like fitbits, heart monitors, and insulin pumps—that allow people to monitor health conditions in real time. It includes connected vehicles—like connected or self-driving cars and drones—that are believed will greatly reduce traffic accidents and may even reduce pollution through less fuel use or drivers relying on car sharing.[11] It even reaches smart home products—like monitoring systems, thermostats, HVACs, refrigerators, and coffee makers—that will help

9. *Id.* at 3.

10. The United Nations' Broadband Commission estimates that 4.2 billion people do not have regular Internet access. Lulu Chang, *On the Web Right Now? You're in the Minority—Most People Still Don't Have Internet*, DIGITAL TRENDS (Sept. 24, 2015, 2:02 PM), http://www.digitaltrends.com/web/4-billion-people-lack-internet-access/.

11. Camille von Kaenel, *Driverless Cars May Slow Pollution*, SCI. AM. (Jan. 19, 2016), https://www.scientificamerican.com/article/driverless-cars-may-slow-pollution/#.

you manage your home and keep an eye on your kids or house while you're away.

And that is just on the consumer side. On the business or industrial side, companies are now able to automatically manage inventory using connected scales and the Cloud, saving both time and money; office buildings can benefit from technology that reduces elevator wait time by predicting demand patterns, saving employees and visitors time, and building management money and energy; and sensors can be used to monitor rail equipment and gas lines to alert engineers of maintenance needs, ultimately increasing safety.

And let's not forget the "smart cities" that are searching for ways to use technology and connectivity to make cities more livable and efficient through things like reducing traffic congestion or saving money and energy through the use of automated street lights or sensors to do things like alert when trash needs to be removed.[12]

But while increased connectivity has vast benefits, it also presents serious privacy and security risks. For reasons I will discuss in greater detail in a moment, many, if not most, of these devices may be vulnerable to outside attacks. These vulnerabilities, when exploited, can cause serious harm to consumers and the country as a whole.

So what are these harms? There are obviously the traditional consumer privacy concerns. Vulnerabilities could be exploited to obtain personal, potentially sensitive, data about consumers. These devices by design collect and maintain massive amounts of data about the users. Take fitness trackers for example. Not only do they count your daily steps, but they can also monitor your sleeping habits, including what time you went to bed and how long you stay asleep. This could potentially provide evidence of sleep disorders or a period of high stress in your life—or possibly even help marketers to identify new parents! Connected cars will inevitably be a treasure trove of information, not just about your whereabouts, but also about your driving habits and your willingness to take risks. Are you a frequent speeder? Or, could you be deemed a risk taker based upon your frequency to let your gas tank hit empty before refueling?

And while traditional privacy concerns are serious enough, the types of devices that are now able to be connected have the potential to allow far more nefarious results, such as the ability to facilitate the attack on other systems. I'm sure most of you recall last fall's DYN attack that severely slowed or

12. Andy Boxall, *When Cities Adopt Smartphone Chips, Trash Cans Talk and Street Lamps Have Ears*, DIGITALTRENDS (Jan. 23, 2015, 1:10 PM), https://www.digitaltrends.com/mobile/how-smartphone-chips-are-connecting-cities/.

stopped services like Twitter, Netflix, Spotify, and other popular sites.[13] For those of you who are not familiar, last October, attackers were able to exploit vulnerabilities in unsecured baby monitors and webcams to perpetrate a Distributed Denial of Service—or DDoS—attack. This is when multiple systems are compromised in order to flood a network with traffic, essentially shutting it down. This attack only lasted for a brief period, but it was a good reminder of the massive impact unknown and unpatched vulnerabilities can have on the entire network.

The variety in types of devices that are now connected to the Internet could also potentially pose serious safety and health risks if hacked. I'm sure you all recall the jeep hacking that was widely publicized in the fall of 2015.[14] In that instance, a team of researchers were able to hack into a jeep through the radio system while a reporter was on the highway and the hackers were able to tamper with the breaks. Imagine if that happened on a busy highway to an unsuspecting driver, or worse, to multiple vehicles simultaneously.

Or pacemakers. Just a couple months ago, the Food and Drug Administration issued a public safety notice confirming the possibility that hackers could "remotely compromise security" and change commands to certain pacemakers and implantable defibrillators while still wired to a patient's heart.[15] A security patch is ready to address this specific problem, but these reports should remind us all of the potential for devastating results as more and more devices rely upon interconnectivity to function.[16]

As more and more devices are connected and consumers and businesses become more dependent upon these devices for their day to day lives, the challenge that we must confront is how to harness all of the benefits of this great innovation, while at the same time protecting consumers from harms—some of which we cannot even fathom yet.

And let me be clear, by "we" I don't just mean "we the government," I mean "we the people";

We the consumer;

We the industry;

---

13. Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. TIMES (Oct. 21, 2016), https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0.

14. Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

15. Safety Communication, Food & Drug Admin., Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication (Jan. 9, 2017), https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.

16. *See, e.g.*, Joe Carlson, *FDA Says St. Jude Heart Devices Vulnerable to Hacking*, STAR TRIB. (Jan. 10, 2017, 12:07 PM), http://www.startribune.com/fda-says-st-jude-heart-devices-vulnerable-to-hacking/410153595/.

We the nation.

Everyone needs to participate and do their part.

So, what do *we* need to do and how do *we* do it together?

First, we need to recognize and accept that there will never be perfect security. I know, this is a truism to anyone in the privacy and security space. But the privacy and security challenges in the IoT space are magnified by a significant distinction from the traditional computer and phone challenges: namely, IoT devices are not designed or expected to be disposed in a few years, unlike, say, the last smartphone model. These IoT devices, like a home security system or a connected car, have much longer shelf lives. So when I told you earlier that in 2003 there were 500 million IoT devices and in 2010 that number had exploded to 12.5 billion and that this number is expected to continue to expand exponentially, what I am communicating to you now is not only will we have to confront the privacy and security challenges of each of those devices, but, more importantly, that those devices are here and likely to be around for a long time, probably even after the manufacturers of those devices have ceased supporting them because they have other business priorities or may have even gone out of business.

And, let's also be clear, these devices have no borders. They can be manufactured by a company in Uzbekistan for use by consumers in Uzbekistan, but it is very probable that many of those devices will find their way across the world. Thus, even if we can find regulatory solutions to these privacy and security challenges for IoT devices that enter commerce in the United States, how will we deal with the flow of these devices from other countries?

Folks, these are the kinds of cyber policy challenges that we are facing with the IoT. What we truly need are solutions that minimize the risks and incentivize all actors involved to take responsibility, including consumers, manufacturers, and Internet Service Providers ("ISPs").

Let's take a look at these incentives in the context of the Internet of Things. On the consumer side—and this is not meant to sound like a criticism of consumers—these devices are designed to be mainstream, but the security of them can be highly technical. Security breaches and vulnerabilities often do not impact the utility of the device. If a consumer does not notice an immediate impact on the user experience, they likely will never know to look for a problem. That is, if the device is still working, consumers likely will not notice that the device has been compromised or could be compromised. This is what happened in the DYN attack last fall, as an example. Consumers who had baby monitors were still able to use those monitors without any noticeable interruption. We simply cannot assume, however, that we are safe because we do not notice a problem.

Similarly, we have to recognize that device manufacturers may not be fully incentivized to protect consumer privacy. As I just mentioned with respect to consumers, compromised devices continue to work as intended. If a device is still working as intended, there is less of an incentive for device manufacturers to proactively address security vulnerabilities, which sometimes might be quite costly. The relative lack of incentives for device manufacturers is also complicated by the ease with which these devices are used or transferred around the world. Further, device manufacturers cannot be relied upon to commit to maintaining the security of devices in perpetuity, and this is particularly true for those manufacturers who go out of business. But, frankly, the bigger issue that we face with device manufacturers is that while every company these days has become a quote-unquote "tech" company by having a website, mobile app, or connected product, not every company has become a security company by building security into their product design and consistently monitoring and patching cyber threats that might affect their products.

Finally, we also have to recognize the role of network providers, such as ISPs, in preventing and responding to cyber threats. Unfortunately, it seems that many ISPs are not proactive given that the majority of the exploits do not directly impact the networks. But the ISPs have good visibility into their network traffic and are in a unique position to help safeguard the networks and those devices connecting to it. In Australia, for example, the Australian Communications and Media Authority—essentially the FCC of Australia—has partnered with ISPs to launch an innovative cyber initiative called the Australian Internet Security Initiative, which is intended to help reduce malware and security vulnerabilities in Australia.[17] Through this voluntary public-private partnership, participants voluntarily share potentially vulnerable IP addresses with ISPs through daily email reports. The ISPs are then "encouraged" to alert affected customers about the vulnerabilities and offer guidance on ways to fix the vulnerabilities or otherwise secure the devices.[18] While nothing like this is yet in the works in the United States, opportunities like this may exist and should be explored here.[19]

In addressing cyber security in the Internet of Things, we need to find a way to guarantee that IoT devices are easily updated to protect against current threats. For many IoT devices, software updates from manufacturers are intermittent—if at all. Admittedly, there are reasons for this. Many of these

17. *Australian Internet Security Initiative*, AUSTRALIA COMMC'NS & MEDIA AUTH., http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative (last updated May 22, 2015).

18. *Id.*

19. *See* Priscilla M. Regan, *Reviving the Public Trust Concept and Applying It to Information Privacy Policy*, 76 MD. L. REV. 1025, 1037–43 (2017) (arguing that a public trustee type of regulatory regime should be imposed on "edge players" such as Facebook and Google).

products have a long shelf life or are one-time only purchases. For example, consumers may replace their iPhone every two years or so once the new and improved version is released. However, other IoT devices, such as connected toasters, for example, are rarely replaced. For industry, some connected devices, such as the elevators that I mentioned earlier or conveyor belts in a factory, are rarely, if ever, replaced. On the flip side, some devices are very inexpensive and therefore easy to replace with newer versions, so manufacturers may not have an incentive to provide costly updates. And, in certain situations, updates for devices may be impossible. Once technology expands to the point where certain devices are no longer supported, despite consumers and business continued use, updates and patches may be impossible for the manufacturers to provide. But these rationalizations do not eliminate the risks and, therefore, as long as the risks exist, we collectively need to address them.

We also need to ensure that consumers are sufficiently informed. Securing devices often relies upon consumers who may not be aware of vulnerabilities or even realize that these devices are even connected to the Internet—let alone vulnerable and in need of updates or continued maintenance.

We undoubtedly face many challenges as we work towards these goals. One such challenge is fragmentation. The Internet of Things will continue to impact every aspect of consumers' lives—healthcare, education, transportation, public safety, and the list goes on and on. As a result, on the government side, multiple agencies play a role: the Federal Communications Commission, the Federal Trade Commission ("FTC"), the Food and Drug Administration. I could continue, but I imagine you all get the point.

With such a vast variety of devices to consider—so many varying needs, collections, and uses of consumer information, so many different existing laws and policies, and the assorted interests of many government entities to consider—whether and how best to regulate is a challenge.

Let's look at an example, say connected cars. The National Highway Transportation Safety Administration or NHTSA is primarily concerned with the safety aspects of connected cars. The NHTSA would investigate how to prevent hacking for safety purposes, such as to prevent hackers' access to and control of essential functions and features of the cars or to otherwise protect drivers on the road. The FTC would focus on the masses of customer information, including vehicle statistics and detailed information on drivers' habits and locations that will inevitably be collected and stored. This type of information is likely of great interest to marketers, and the parameters around how this information can be shared will also be of great interest to the FTC. Finally, there is law enforcement. These cars will have collected so much

information that may be valuable in investigations. How can law enforcement obtain access to that data?[20]

Fragmentation is also a concern on the industry side. Now every company is essentially a tech company, yet they often lack the background or expertise to properly implement strong data security and privacy protections at the outset.

The Internet of Things is still in its infancy. And while it has certainly exploded over the last few years, the full extent of what can and will be connected is still unknown. Government administrative and legislative processes are slow. In an area such as IoT that is rapidly developing, even if the government were able to get a regulatory plan in place quickly, it would likely be outdated in six months. The ability for the government to keep any laws or regulations up to date as new technologies develop is another challenge—and frankly a real concern. Also, we need to be mindful that this is a global problem, which means that even if we were able to craft regulations or standards in the United States, this would not cure the problem. Further, the devices themselves are likely to cross borders. Today, it is just as easy to purchase a smartphone from the store down the street as it is to purchase one on eBay and other Internet sites. Devices manufactured abroad may neither contain similar security protections nor be compatible with any efforts taken to provide software updates and patches in our home country.

So what can we do?

To start, what is the government's role? In areas of innovation, people often fear government involvement. So I think that it is important to dispel this myth that all government involvement or regulation is *per se* harmful to innovation. In fact, government involvement can often be helpful to put everyone on equal ground and ensure consumers are able to use the services and devices that they want to use, and prohibit companies from limiting consumers' uses. Moreover, the role of government in this space goes well beyond traditional regulatory practices of promulgating and enforcing administrative rules. Additionally, the

- government plays a role in education.
- government plays a role in promoting best practices.
- government plays a role in defending us from attacks.
- government plays a role in holding those accountable who engage in such attacks.

Each of these is just as important as promulgating and enforcing regulations.

20. *See, e.g.*, Markus Rauschecker, *Rule 41 Amendments Provide for a Drastic Expansion of Government Authority to Conduct Computer Searches and Should Not Have Been Adopted by the Supreme Court*, 76 MD. L. REV. 1085 (2017) (discussing amendments to the Federal Rules of Criminal Procedure to facilitate law enforcement's ability to target individuals who use computers to perpetrate crime).

Over the past few years, the federal government has focused a great deal of energy and resources in this area, with the goal of being proactive rather than reactive. Yes, they have been working to implement new rules and regulations when needed and enforcing existing ones where appropriate, but the government has also hosted workshops and held hearings, engaged in multi-stakeholder processes, issued reports and other guidance for industry, and even put challenges to the technology community to attempt to entice creative solutions.

Industry obviously plays a vital role in securing devices that they make available. Industry needs to not only focus on privacy and security as early as the development phase—what has been dubbed "privacy by design" or "security by design"—but also throughout the life of the device and beyond if necessary.[21]

When we say privacy or security by design, what we generally mean is that industry needs to implement reasonable privacy and security processes from the outset, not just react once things go wrong. The FTC, among others, has stressed this notion repeatedly: that in order for consumers to adopt these technologies, they need to trust them.[22] Therefore, industry needs to consider the privacy and security implications as early in the process as possible. Simple things like randomizing default passwords will go a long way to prevent incidents like the recent DDoS attack.

Further, I want to highlight an issue with maintenance throughout the life of the device. In this new interconnected world, vulnerabilities are going to reveal themselves. Industry, including manufacturers and network operators, needs to routinely monitor for vulnerabilities and expeditiously address detected vulnerabilities and issue patches or updates when feasible. Industry could also benefit from coming up with creative solutions for providing support even after the life of device.

And we must not forget the important role that industry plays in educating consumers. Consumer education is vital. Companies today most often communicate with consumers through privacy policies that inform proactive consumers (who read them) what data is collected and how the information is used or shared. But industry needs to do more to educate consumers on the risks of connected devices and what security mechanisms are available, and also to reach those consumers that may not be as proactive.

21. Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 980 (contending that "[p]rivacy law should more explicitly address the design of consumer technologies").

22. Margot E. Kaminski, *Averting Robot Eyes*, 76 MD. L. REV. 940, 984 (2017) (arguing in the context of robots in the home: "if home robots are to be widely trusted, accepted, and adopted, roboticists will need to build them with privacy in mind").

On that note, finally today I would like to mention the role of the consumer. There is no doubt that industry needs to implement reasonable security and government needs to do its part. But, consumers play an important role too in both protecting their own privacy and ensuring that available security features are used. Consumers need to be made aware of how best to protect themselves and then take the necessary precautions, including changing factory passwords, using only secure Wi-Fi networks, and downloading or installing available patches and updates.

We are embarking on a whole new world. A world where eventually everything will be able to be connected. This undoubtedly presents many benefits and opportunities to both consumers and industry—some that we are already recognizing and far more that we cannot even imagine yet. It would be a travesty for these great benefits to not be realized because we all failed to pay attention to the very real and very serious privacy and security issues that growing interconnectedness presents. We are at the forefront of a very exciting new reality, and it is on all of us to work together and ensure that we do all we can now to guarantee safety and security for the future.

Thank you.