Opening Keynote for Inaugural Meeting of the Privacy Bar Section of the IAPP
Julie Brill
Hogan Lovells
April 7, 2016

Good morning. I am pleased to help kick off the IAPP's Privacy Bar Section today, and it is a privilege to follow the welcoming remarks by Chris Wolf and Trevor Hughes. Chris and Trevor are leaders in the effort to build a community of privacy practitioners in companies and governments around the world, to integrate academics and advocates into the discussion, and to train the next generation of privacy leaders. The establishment of the Privacy Bar Section is a testament to their vision and commitment to the value of privacy.

The growth of privacy law also has a lot to do with the rise of the commercial Internet. The Internet has become today's global trade route, and personal data is one of its major currencies.[1] The growth in the digital economy is impressive. One study found that economic activity taking place over the Internet is growing at 10% per year within the G-20 group of nations.[2] So is its overall size in absolute terms. To take one measure, the Department of Commerce reported in 2014 that the U.S. exported nearly $360 billion in digitally deliverable services, and that the national surplus in such services was about $135 billion.[3]

Much of this economic activity depends on exchanges of personal information, and that makes appropriate privacy and security protections essential. This means that our work here, as members of the Privacy Bar Section of the IAPP, is hugely important. The issues that arise regarding personal information and the digital economy are going to increase not only in scale but also in complexity in the coming years. As practitioners in this area, it is our job to look around the corner and to anticipate the upcoming challenges; to work together to create practical and executable solutions; and to be vigilant leaders in what will continue to be a constantly changing field.

One challenge that has faced the digital economy for some time now is its dependence on exchanges of personal information and its relationship with the individual consumer. Consumers want to know – and should be able easily to find out – what information companies are collecting, where they're sending it, and how they're using it. This kind of information is important to consumers' decisions not only about how to use digital products and services, but also whether to use them in the first place.

My former agency, the Federal Trade Commission (FTC) was quick to understand this connection. The FTC's actions in the privacy space generally are also something that members of the Privacy Bar Section will continue to watch very closely. With the Section's opening as a backdrop, I would like to share a few of my thoughts about the FTC's future in privacy enforcement, policy, and international engagement. My hope is that these remarks will serve as initial food for thought as we join together as the new Privacy Bar Section in supporting future growth and innovation, imbued with the values of privacy.

Enforcement

The FTC entered the privacy and data security arenas because the potential for security breaches and misuses of personal information to harm consumers was clear. Over the past 20 years or so, the Commission has brought around 100 actions solely under section 5, protecting

millions of consumers – in the United States, Europe, and elsewhere – from deceptive or unfair data practices.

Although the FTC has never been alone on the privacy frontier, other agencies have arrived on the scene or recently begun to take on more prominent roles. The FCC[4] and CFPB,[5] for example, have adopted more aggressive enforcement and regulatory positions. The states, which have been active privacy and data security enforcers all along, have passed many of their own laws, ranging from law enforcement access, to biometrics and drones, to revenge porn. And the European Union (EU) and Member State DPAs have exerted a constant influence on companies' data practices and on broader debates about what protections privacy laws should offer and how to put those protections into practice.

Yet the FTC, with its broad authority under Section 5,[6] will be an increasingly important force as technology develops, and the silos that sector-specific laws are built around begin to crumble. Take health information as an example. The federal health privacy law, HIPAA, is a crucial source of privacy protections for consumers in traditional healthcare settings. But the booming popularity of wearable health devices, health apps, and health-related websites has made it clear that a lot of information that is just as sensitive as what our physicians collect escapes HIPAA's purview, and flows freely without the same protections that apply in hospitals and doctors' offices.[7] The FTC's authority provides an important source of protection for such health information that flows outside of the HIPAA context. As the digital economy and innovative service offerings to consumers grow, more sensitive information will seep through the sector-specific barriers and protections that we have set up. The FTC's net of protection can capture the information that falls through the cracks. I expect the FTC to rely upon its unique authority and broad jurisdiction to find ways to take action when consumers' sensitive data is lost or misused.

Another hallmark of FTC enforcement in recent years has been the speed with which the agency has used its existing authority to address privacy concerns that sometimes accompany new technologies. Social networks,[8] messaging apps,[9] connected devices, and location analytics services[10] have all been subject to FTC enforcement actions under Section 5. The signal that these cases send is clear: new services and technologies do not receive a pass from the FTC.

But the FTC often addresses emerging practices with something short of an enforcement action. Warning letters play an important role in alerting companies about potentially illegal practices. And because, such letters can precede enforcement actions, as was the case with FTC warning letters to mobile app vendors with respect to COPPA[11] and Fair Credit Reporting Act[12] issues, these warning letters send broader signals to the market. Last month, FTC staff sent 12 warning letters to app vendors that use a software development kit that apparently allows apps to track consumers' television viewing habits by detecting unique audio codes placed in programs or ads.[13] The letters encourage the app vendors to determine whether their use of the software in question enables third parties to monitor consumers' television viewing habits and, if it does, to effectively inform consumers so that they can decide whether to use those apps. We will have to wait to see whether the FTC's most recent warning letters lead in a similar direction.

The concerns that underlie these warning letters are similar to those in the FTC's actions against Path,[14] Aaron's,[15] and DesignerWare[16]: If a company is going to collect or use information – especially sensitive information – in a completely unexpected way, it needs to be very clear about it with consumers.

Another way the FTC has addressed the impact of new technologies is through workshops on cutting edge issues like cross device and retail mobile location tracking. Indeed, just last week, the FTC announced a three-part fall technology series that will address smart TVs, drones, and ransomware.[17]

I expect the FTC to continue to use the enforcement mechanisms at its disposal to swiftly and adeptly react to potential consumer harms related to emerging technologies and spaces. As a Privacy Bar Section, we can stay up-to-date not only on the content of enforcement actions but also on FTC warning letters, workshops, and other activities, in order to maintain our thought leadership and ability to participate in these important discussions about privacy.

Big Data and the Internet of Things

These enforcement actions, warning letters and workshops present various slices of the broader issues that confront consumers, companies, and enforcement agencies like the FTC as our society embraces connected devices and increasingly powerful data analysis tools. The FTC has been a leader in thinking holistically about the potential benefits and risks of the Internet of Things and big data, and for the past few years it has been conducting a broad and deep conversation about the roles of privacy and security in these emerging technologies.

The promise of these technologies is significant. Cities can better maintain their infrastructures by developing sophisticated early warning systems for gas and water leaks. Medical researchers can enroll patients in large-scale research projects and collect streams of useful, reliable data that in the past would have been a mere trickle from surveys and patients' own reports.[18] And the prospects for connected devices to help companies run their operations more efficiently seem nearly endless.

But the challenges are significant. More devices in consumers' homes, cars, and even clothes will mean much more sensitive data will be collected. User interfaces on devices will shrink or disappear, making it more difficult for consumers to know when data is being collected, let alone exercise any control over the collection itself. Connectivity will just be part of how things work, as electricity is today.

And the data that will be available as a result of these connected devices will be deeply personal. Some of these devices will handle highly sensitive information about consumers' health, homes, and families. Some will be linked to consumers' financial accounts or email accounts. And all of this sensitive data will feed the burgeoning data analytics industry and new kinds of algorithmic decision-making.

Security is one of the biggest challenges with the Internet of Things, and security is essential to privacy. Unfortunately, there is some evidence that security vulnerabilities are rampant in the Internet of Things. A study by Hewlett-Packard found that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data without encryption.[19]

And because many connected devices are linked to the physical world, *device* security also is a top concern. But many connected devices will be inexpensive and essentially disposable. If a vulnerability is discovered on such a device, will such manufacturers have the appropriate economic incentive notify consumers, let alone patch the vulnerability?[20]

Over the past few years, the FTC has made a significant effort to draw attention to the importance of security in the Internet of Things and to provide more specific guidance about what it expects from companies that provide IoT devices and services. This guidance has taken the form of the 2015 staff report on the IoT,[21] a detailed blog post on specific IoT security considerations,[22] and a series of *Start with Security* workshops that have been held, so far, in San Francisco,[23] Austin,[24] and Seattle.[25]

A basic premise of the reasonable security standard that the FTC enforces is that it requires companies to be aware of the amount and sensitivity of personal data that they process, and to take security measures that are appropriate for the data and for the size and complexity of their businesses.[26] The FTC also expects ongoing assessments to be part of a continuing process of identifying new risks and adjusting their security practices accordingly. Since data security risks differ for each company, no single prescription for a security process or program will work for all companies.[27]

The FTC has heard the call from companies to be more specific about what "reasonable security" requires, and has responded, though perhaps not as quickly or in as much detail as some companies would like. A couple of developments in this space will be worth watching very closely. First, the FTC's settlement with Wyndham requires the company to meet a "PCI+" standard for the cardholder data that it handles.[28] That is, Wyndham will be deemed to comply with the final order's comprehensive information security program if it passes annual audits conducted by an independent, qualified, conflict-free auditor; and the auditor certifies the extent of Wyndham's compliance with PCI's Risk Assessment Guidelines.

The *Wyndham* order depends heavily on independent PCI audits, and this leads to the second development that practitioners should watch closely over the next couple of years. Last month, the FTC ordered nine companies that conduct PCI DSS assessments to file so-called "special reports" issued under the agency's 6(b) authority.[29] The orders focus heavily on these firms' independence by examining their incentives, procedures, and interactions with clients.[30] Given the role that PCI assessments play in *Wyndham* and other data security orders and in the greater scheme of protecting payment card information, this focus makes sense.

Privacy Shield and the Merging "Lanes" of Privacy

The FTC and U.S. stakeholders are not the only ones wrestling with the many privacy and security issues raised by the Internet of Things and big data. Companies and regulators in Europe are confronting them, too, and all involved would benefit from a deeper and more sustained discussion. This is particularly true now that the effective date for the General Data Protection Regulation (GDPR) is just about nailed down, and many of its provisions – such as privacy by design, data security, and a stricter definition of consent – require careful thought to implement in connected devices and the data-intensive services that go along with them.

For much of the past few years, however, and certainly for the past six months, these discussions have taken a back seat to the more immediate issues surrounding Safe Harbor and transatlantic data transfers more generally.

The EU-U.S. Privacy Shield[31] settles – for now – the questions about what will replace Safe Harbor. Privacy Shield repairs the two greatest losses that the European Court of Justice's

invalidation of Safe Harbor inflicted: the loss of transparency that would have come from pushing thousands of former Safe Harbor companies to rely on binding corporate rules and standard contractual clauses, and the loss of FTC enforcement.

These two issues go hand-in-hand, since it is the public commitment of companies to provide the protections that were spelled out—first in Safe Harbor, and now in Privacy Shield—that provides the easiest hook for FTC enforcement. The FTC has committed to continuing to vigorously enforce the Privacy Shield principles, and it will be joined by the Commerce Department and the European DPAs in that effort. Privacy Shield also requires stronger commitments on the part of third-party controllers and agents.[32] In addition, Privacy Shield includes a raft of new procedural rights that will allow consumers to pursue complaints against participating companies,[33] and the FTC reaffirmed its commitment to give priority to referrals from European DPAs.[34] Add to this the strong protections that Privacy Shield requires with respect to sensitive information, access, and other fundamental privacy protections. All of these elements together provide strong substantive protections, practical individual redress mechanisms, and effective oversight and accountability through the efforts of the FTC, Department of Commerce, DPAs, and the European Commission.

And all of this is before we consider Privacy Shield's commitments on law enforcement and intelligence agencies' access to personal information held by Privacy Shield companies. I will not go into the details of these commitments today. Instead, I would like to draw attention to the fact that these commitments exist alongside those from the FTC and the Department of Commerce in the same framework.[35] This speaks volumes about the extent to which the different privacy silos, or "lanes" as they're known in the government, have begun to merge. We can see further evidence of this merging of commercial issues and government access issues in areas such as ECPA reform and the use of encryption in commercial products and services.

There is a role for the FTC to play in debates about encryption and reform of the Electronic Communications Privacy Act because the FTC's combination of privacy and data security enforcement experience, and increasing technical sophistication, give it a unique perspective in these discussions.[36] Whether my former colleagues at the Commission, and future Commissioners, will seek a more prominent role in these debates is something that remains to be seen.

There is a lesson in all of this for you as inaugural members of the Privacy Bar Section. The Section's creation marks the recognition that privacy law is here to stay. But we know that does not mean that it will stay the same. As practitioners, we all need to be aware of how changes in technology, business practices, and – I don't think I'm making an overstatement – political developments in the U.S. and elsewhere affect companies, consumers, and regulatory and enforcement agencies.

I expect the Privacy Bar Section to help us think more deeply about how the law – and enforcement of the law – will develop in light of all of these challenges. I look forward to working with all of you to contribute to the effort.

Thank you.

---

[1] William E. Kennard, U.S. Ambassador to the EU, Winning the Future Through Innovation, Remarks Before the AmCham EU Transatlantic Conference (Mar. 3, 2011), *available at* http://useu.usmission.gov/kennard_amchameu_030311.html.

[2] World Econ. Forum, DELIVERING DIGITAL INFRASTRUCTURE: ADVANCING THE INTERNET ECONOMY 7 (Apr. 2014), *available at* http://www3.weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Report_2014.pdf.

[3] Dept. of Commerce, Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services 2 (Jan. 2014), *available at* http://www.esa.doc.gov/sites/default/files/digitaleconomyandcross-bordertrade.pdf.

[4] *See, e.g.*, FCC, Press Release, FCC Settles Verizon "Supercookie" Probe (Mar. 7 2016), *available at* https://www.fcc.gov/document/fcc-settles-verizon-supercookie-probe; FCC, Agenda for March 2016 Open Commission Meeting (noting that the Commission will consider a Notice of Proposed Rulemaking concerning privacy rules for broadband Internet access service providers).

[5] *See* CFPB, Press Release, CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices (Mar. 2, 2016), *available at* http://www.consumerfinance.gov/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[6] *See* 15 U.S.C. § 45.

[7] *See* FTC, Press Release, Spring Privacy Series: Consumer Generated and Controlled Health Data (May 7, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.

[8] *See* Google, Inc., C-4336 (F.T.C. Oct. 13, 2011) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf *and* Facebook, Inc., C-4365 (F.T.C. July 27, 2012) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf/.

[9] Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf.

[10] FTC, Press Release, Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices (Apr. 23, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers.

[11] *See* FTC, Press Release, FTC Sends Educational Letters to Businesses to Help Them Prepare for COPPA Update (May 15, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/05/ftc-sends-educational-letters-businesses-help-them-prepare-coppa; FTC, Press Release, Yelp, TinyCo Settle FTC Charges Their Apps Improperly Collected Children's Personal Information (Sept. 17, 2014), available at https://www.ftc.gov/news-events/press-releases/2014/09/yelp-tinyco-settle-ftc-charges-their-apps-improperly-collected.

[12] *See* FTC, Press Release, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/02/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting; FTC, Press Release, Marketers of Criminal Background Screening ReportsTo Settle FTC Charges They Violated Fair Credit Reporting Act (Jan. 10, 2013), available at https://www.ftc.gov/news-events/press-releases/2013/01/marketers-criminal-background-screening-reportsto-settle-ftc.

[13] *See* FTC, Press Release, FTC Issues Warning Letters to App Developers Using 'Silverpush' Code (Mar. 17, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

[14] *See* FTC, Press Release, Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.

[15] *See* FTC, Press Release, Aaron's Rent-To-Own Chain Settles FTC Charges That It Enabled Computer Spying by Franchisees (Oct. 22, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer.

[16] *See* FTC, Press Release, FTC Halts Computer Spying (Sept. 25, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/09/ftc-halts-computer-spying.

[17] *See* FTC, Press Release, FTC to Host Fall Seminar Series on Emerging Consumer Technology Issues (Mar. 31, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/03/ftc-host-fall-seminar-series-emerging-consumer-technology-issues.

[18] *See, e.g.*, Jenna Wortham, *We're More Honest with Our Phones than with Our Doctors*, N.Y. TIMES (Mar. 31, 2016), *available at* http://www.nytimes.com/2016/03/27/magazine/were-more-honest-with-our-phones-than-with-our-doctors.html; Elizabeth Whitman, *Apple ResearchKit: Is New Open-Source Software for Sales or the Greater Good of Health Care*, INTL. BUS. TIMES (Mar. 16, 2015 3:51 PM), *available at* http://www.ibtimes.com/apple-researchkit-new-open-source-software-sales-or-greater-good-health-care-1848612.

[19] Hewlett Packard Enterprise, *Internet of Things Research Study* 4 (2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

[20] *See* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 13-14 (2015) (staff report), *available at* http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (discussing views of workshop participants) [IOT REPORT].

[21] *See generally id.*

[22] FTC, Careful Connections: Building Security in the Internet of Things (Jan. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things.

[23] FTC, Press Release, FTC Announces Agenda for First Start with Security Conference in San Francisco (Aug. 19, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/08/ftc-announces-agenda-first-start-security-conference-san.

[24] FTC, Press Release, Federal Trade Commission Announces Agenda for Nov. 5 Start With Security Conference in Austin (Oct. 14, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/10/federal-trade-commission-announces-agenda-nov-5-start-security.

[25] FTC, Press Release, Federal Trade Commission Announces Agenda for Feb. 9 Start With Security Event in Seattle (Jan. 20, 2016), available at https://www.ftc.gov/news-events/press-releases/2016/01/federal-trade-commission-announces-agenda-feb-9-start-security.

[26] *See* FTC, START WITH SECURITY: A GUIDE FOR BUSINESS – LESSONS LEARNED FROM FTC CASES 1 (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

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

[28] *See* FTC v. Wyndham Worldwide Corp., Stipulated Order for Injunction, Case No. 2:13-CV-01887-ES-JAD (D.N.J. Dec. 11, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation.

[29] FTC, Press Release, FTC To Study Credit Card Industry Data Security Auditing (Mar. 7, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing.

[30] *See* Model Order to File Special Report, *available at* https://www.ftc.gov/system/files/attachments/press-releases/ftc-study-credit-card-industry-data-security-auditing/160307datasecurity6border.pdf.

[31] EU-U.S. Privacy Shield Full Text (Feb. 29, 2016), *available at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf.

[32] *See* Privacy Shield Full Text, *supra* note 39, Principles § II.3 ("accountability for onward transfer").

[33] *See* Privacy Shield Full Text, *supra* note 39, Principles § II.7.

[34] *See* Letter from FTC Chairwoman Edith Ramirez to EC Commissioner Věra Jourová, at 5-7 (Feb. 23, 2016) (included in Privacy Shield Full Text, *supra* note 39).

[35] *See generally* Letter from Office of the Director of National Intelligence General Counsel Robert Litt to Justin S. Antonipillai and Ted Dean (Feb. 22, 2016) (included in Privacy Shield Full Text, *supra* note 39).

[36] *See* Julie Brill, Commissioner, FTC, Statement About the Federal Trade Commission's Written Testimony on "Reforming the Electronic Communications Privacy Act Submitted to Senate Judiciary Committee" (Sept. 16, 2015), *available at* https://www.ftc.gov/public-statements/2015/09/statement-about-federal-trade-commissions-written-testimony-reforming.