Federal Trade Commission

Privacy Today and the FTC's 2014 Privacy Agency

Jessica Rich[1]
Director, Bureau of Consumer Protection, FTC

International Association of Privacy Professionals
December 6, 2013

I. Introduction

Hello. I am delighted to be here among so many familiar faces, talking about the important issue of privacy. I want to thank IAPP for inviting me here today.

As we get ready to greet another new year, I can't help but think about how much the world has changed for consumers in the last few decades – and even just the last few years. Not too long ago, cell phones were a novelty. Now, virtually everyone in this country has a mobile device that they take everywhere, and over half of consumers have smartphones.[2]

Companies across many industries are using increasing amounts of data – Big Data – to create better products and services, tailor their messages to consumers in real time, and develop new solutions to nagging global problems. Big Data has the potential to improve the quality of health care while cutting costs; enable forecasters to better predict the weather and spikes in

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner. Special thanks to Molly Crawford for assisting in the preparation of these remarks.
[2] Nielsen Wire, *America's New Mobile Majority: A Look at Smartphone Owners in the U.S.* (May 7, 2012), *available at* http://blog.nielsen.com/nielsenwire/?p=31688.

energy consumption; and improve industrial efficiencies in order to deliver better, and lower cost, products and services to consumers.

Mobile shopping is exploding. Not only can a consumer buy her winter coat while commuting on her train to the office, but she can compare prices, get reviews, conduct a virtual fitting, and have her purchase posted to her social networking page. All of this capability literally sits in the palm of her hand.

Developments in device connectivity also offer many new conveniences and benefits. Wireless medical and fitness devices can not only chart your fitness goals and progress, but also share your latest blood glucose readings with your doctor. And connected cars promise better navigation systems, remote activation of climate control so you are toasty right when you get in your car, and an easy way to find your vehicle in that huge parking lot at Target.

These are incredible developments, and many consumers – myself included – are embracing them. But they also can be unnerving, even scary. Consumers are asking: where is all of my data going? I think the developments with the National Security Agency and Edward Snowden – though they involve government collection of data – has increased consumer concerns about this very good question. Who has my data? Do they need it? Who else can get it? My neighbors? My insurance company? My employer? What can they do with it?

These kinds of questions drive much of what we do at the FTC. Protecting consumer privacy is one of the Commission's most important missions and has been so for over 40 years. Although the Commission's priorities and activities have varied during that time, its central goal has remained constant: to protect consumers' privacy in order to foster trust in the ever-changing marketplace, and in a way that preserves and complements innovation.

Today, I would like to address two particular areas of interest. First, I will discuss why strong privacy and security protections should be important to every business that touches

consumer data. Next, I will talk about the Commission's privacy agenda for the upcoming year. At the end, I would be happy to take your questions.

II. The Importance of Privacy Today

So let's talk about why privacy is – or should be – so important to businesses today.

For many companies in recent years, privacy has simply been a matter of legal and regulatory compliance, best left to lawyers and IT professionals hired to "take care of it." But increasingly, privacy has become a C-suite issue – part of a broader business strategy as consumer awareness and demand for privacy continues to grow.

There is growing evidence of real consumer concern about privacy, and even consumer reluctance to engage fully in the marketplace as a result. Surveys of consumers show not only rising levels of concern but also concrete actions consumers have taken to shield their personal information. For example, a recent Pew study found that 86% of consumers have taken steps to remove or mask their digital footprints.[3] These include steps ranging from clearing cookies to encrypting email, and from consumers avoiding use of their names to using virtual networks that mask their IP addresses. Surveys also show that younger consumers care about privacy, despite assertions to the contrary. In fact, a second Pew survey found that children and teenagers actively engage with their privacy settings on social networks, often set their profiles to privacy-protective settings, and value the control that the settings provide.[4]

Other evidence of consumer concern comes from their reactions to privacy and security breaches when revealed by the company or in the press. Let me take you *way* back to 2005 and the now infamous ChoicePoint breaches. These incidents provided a good lesson about the business impact of poor privacy and security practices. Due to ChoicePoint's allegedly poor

[3] Pew Research Center, *Anonymity, Privacy, and Security Online* (Sept. 5, 2013), *available at* http://pewinternet.org/Reports/2013/Anonymity-online.aspx.

privacy and data security practices, identity thieves were able to obtain highly sensitive consumer information from the company, including Social Security numbers, and perpetrate identity theft affecting at least 800 consumers. The FTC brought a lawsuit against the company that included $10 million in civil penalties and $5 million in consumer redress,[5] but even apart from the FTC"s action, the business cost was significant. The breaches cost ChoicePoint millions, its stock prices fell, and its loss of goodwill was immeasurable.[6] Recall that ChoicePoint is a data broker – a company that generally does not deal directly with consumers – yet the breaches harmed its reputation and business in countless ways.

More recent examples abound. Google's collection of data through Street View, as well as its launch of the Buzz social network using consumers' email contacts to create the service without consent, resulted in not only regulatory inquiries and actions, but also significant backlash from users.[7] And virtually every time one of the large tech companies changes its privacy policy, it creates a huge uproar. For example, Facebook's recent changes to its privacy policy were delayed, and ultimately revised, in part because of public outcry.[8]

These are just some examples of the business impact of a security breach or of failing to adequately consider privacy. Indeed, the FTC has brought actions against numerous companies, large and small, for privacy and security failures that violate the law. For example, earlier this

---

[4] Pew Research Center, *Teens, Social Media, and Privacy* (May 21, 2013), *available at* http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx.

[5] *U.S. v. ChoicePoint*, No. 1:06-CV-0198-JTC (N.D. Ga. Jan. 30, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

[6] *See, e.g.*, Paul Roberts, *ChoicePoint to Stop Some Personal Data Sales*, PC World (Mar. 7, 2005), *available at* http://www.pcworld.com/article/119908/article.html.

[7] *See, e.g.*, Alyssa Newcomb, *Google Hit with $7 Million Fine for Street View Privacy Breach*, ABC News (Mar. 13, 2013), *available at* http://abcnews.go.com/Technology/google-hit-million-fine-street-view-privacy-breach/story?id=18717950; David Streitfeld & Claire Cain Miller, *Google Hastens to Show its Concern for Privacy*, N.Y. Times (Mar. 13, 2013), *available at* http://www.nytimes.com/2013/03/14/technology/google-focuses-on-privacy-after-street-view-settlement.html?pagewanted=all&_r=0.; Clint Boulton, *Google Buzz Privacy Backlash Not Anticipated, Google Says*, eWeek (Feb. 17, 2010), *available at* http://www.eweek.com/c/a/Messaging-and-Collaboration/Google-Buzz-Privacy-Backlash-Not-Anticipated-Google-Says-212091/.

year, we alleged that social networking app Path deceived consumers by secretly capturing and storing contact information from their mobile device address books without their knowledge or consent.[9] Even apart from the FTC's case, there was a huge public outcry about Path.[10] The company suffered loss of goodwill and reputational injury with its users. This is because consumers, competitors, the press, the blogosphere, and others – not just the FTC – pay close attention to privacy and security.

In addition to the negative attention that a privacy or security breach can cause, the opposite is also true – increasingly, we see that improved transparency and consumer choice is a selling point for businesses. Privacy can provide business with a competitive edge. Take, for example, the nation's largest data broker, Acxiom. Acxiom has launched a web-based tool, "About the Data," that allows consumers to view portions of their marketing profile by seeing certain categories of information, like personal characteristics, home, vehicles, household finances (including credit), purchases, and interests.[11] While it still has a long way to go and is by no means a perfect tool, it is a step in the right direction.

In a similar vein, members of groups like the Direct Marketing Association (DMA), Network Advertising Initiative (NAI), and Interactive Advertising Bureau (IAB) have agreed to privacy codes of conduct, even though some of them do not even interact directly with consumers.[12] The cynic would say that this is simply to stave off regulation or government

---

[8] Jessica Guynn, *Facebook Removes Controversial Line About Teens in Privacy Policy*, L.A. Times (Nov. 15, 2013), *available at* http://www.latimes.com/business/technology/la-fi-tn-facebook-teens-privacy-20131115,0,2668591.story#axzz2lOlXWooo.

[9] *U.S. v. Path, Inc.*, No. C-13-0448-JCS (N.D. Cal. Filed Jan. 31, 2013), *available at* http://www.ftc.gov/opa/2013/02/path.shtm.

[10] Gerry Shih, *Path Fumble Highlights Internet Privacy Concerns*, Reuters (Feb. 9, 2012), *available at* http://www.reuters.com/article/2012/02/09/us-socialmedia-privacy-path-idUSTRE81826X20120209.

[11] *See generally* https://aboutthedata.com/.

[12] Direct Marketing Association, *DMA OBA Guidelines*, *available at* http://thedma.org/issues/dma-oba-guidelines/; Network Advertising Initiative, *The NAI Code and Enforcement: An Overview*, *available at* http://www.networkadvertising.org/code-enforcement (last visited Nov. 22, 2013); Interactive Advertising Bureau, *IAB Code of Conduct*, *available at* http://www.iab.net/codeofconduct (last visited Nov. 22, 2013).

oversight – and, yes, I am sure that's part of it. But companies also sign on to these codes because they think privacy is a selling point with both consumers and their business clients.

Finally, as I think everyone in this audience knows, privacy is critical as we move to an increasingly global economy where data must flow between different privacy regimes for commerce to thrive. This is precisely what the US-EU Safe Harbor is all about – adhering to broadly accepted privacy principles in order to allow data to flow between the US and the EU, which is particularly critical for multinational corporations.[13] This is also why the FTC is working on cross border rules through APEC, which establishes a system of accountability when companies transfer data across national borders.[14] Global frameworks like these are what businesses need to broaden their customer base in the global market, and also to efficiently manage day-to-day operations all over the world.

All of this is mounting evidence that companies can leverage consumers' demand for privacy as part of a broader business strategy. One of the greatest assets a business has is the trust of its customers. Companies that get ahead in privacy – and I should stress that I mean *real* privacy and not just empty promises – can get ahead with consumers.

III. The FTC's Privacy Agenda

Not surprisingly, privacy is a top priority for the Commission. We promote strong privacy protections using all of the tools at our disposal – enforcement, workshops, studies, reports, and consumer and business education and outreach. Over the past few decades, the Commission has brought hundreds of privacy and data security cases targeting violations of the Federal Trade Commission Act, the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act, Do Not Call, CAN SPAM, and the Children's Online Privacy Protection Act (COPPA).

---

[13] *See generally* http://export.gov/safeharbor/eu/eg_main_018365.asp.

Since just 2001, the Commission has brought 44 privacy cases, 47 data security cases, and 21 COPPA cases. We've brought high-profile cases against companies like Facebook, Google, Microsoft, and ChoicePoint; cases against smaller companies engaged in practices of particular concern; and cases challenging unfair and deceptive uses of cutting-edge technology.

The Commission also has distributed millions of copies of educational materials for consumers and businesses to improve their understanding of ongoing threats to security and privacy. And the FTC continues to examine the implications of new technologies and business practices on consumer privacy through ongoing policy initiatives.

We have no intention of slowing down. Our privacy work will continue at a rapid pace in the coming year. We have a full agenda, which can best be described in three basic – and in many ways, overlapping – categories: Big Data; Mobile Technologies and Connected Devices; and Protections for Sensitive Data.

A. Big Data

The first area of focus I will discuss is the phenomenon of Big Data, a phrase that seems to be in vogue when discussing the vast capabilities of companies to gather data from numerous sources and "crunch" it to make inferences about people. Big Data can, of course, drive valuable innovation – for example, it can be used to track traffic patterns in order to ease congested commutes home, or even determine what medical treatments are most effective across a large population. However, the pooling of vast stores of data raises obvious consumer privacy concerns. These concerns stem from the risk of indiscriminate and virtually unlimited data collection without consumer knowledge or consent; the risk of data breaches involving this

[14] *See, e.g.*, FTC Press Release, *FTC Welcomes a New Privacy System for the Movement of Consumer Data Between the United States and Other Economies in the Asia-Pacific Region* (Nov. 14, 2011), *available at* http://www.ftc.gov/opa/2011/11/apec.shtm.

treasure trove of information; or the risk that companies will make inferences about consumers that simply are not true.

Our activities on the Big Data front will include the release of a report on data brokers in the coming months. This is an area of particular concern for the FTC. As the Commission has discussed in reports and testimony, data brokers collect, maintain, and sell a wealth of information about consumers, but they often do not interact directly with consumers.[15] Rather, they get information from public records and purchase information from other companies. As a result, consumers are often unaware of the existence of data brokers, as well as the purposes for which they collect and use consumers' data.

This lack of transparency means that even when data brokers offer consumers the ability to access their data, or provide other tools, many consumers do not know how to exercise this right. Unless data brokers use consumer data for credit, employment, insurance, housing, or other similar purposes,[16] there are no general laws requiring them to maintain the privacy of that data. The primary purpose of the upcoming report is to shine a light on the data broker industry and increase transparency and awareness about its practices.

Of course, Big Data is not limited to the data broker industry. Ad networks, ISPs, social networks, operating systems, and others also have the capability of collecting and analyzing Big Data. Last year, we held a workshop that examined what we call "comprehensive data collection" – the ability of certain companies like ISPs, social networks, or multi-service companies to track consumers comprehensively and continuously over time, across multiple sites

---

[15] *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf ("Privacy Report"); Prepared Statement of the FTC, *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission: Hearing Before the S. Comm. on Commerce, Science, and Transp.*, 112th Cong. (May 9, 2012), *available at* http://ftc.gov/os/testimony/120509privacyprotections.pdf.

[16] The Fair Credit Reporting Act imposes obligations on consumer reporting agencies, furnishers, and users of information used by issuers of credit, insurance companies, employers, landlords, and others in making eligibility decisions affecting consumers. *See generally* 15 U.S.C. §§ 1681-1681x.

or even across multiple devices, and at a high level of detail.[17] We are working to finalize a report based on our findings from the workshop, and expect to release it in the coming months.

In addition, as we announced just this week, we are planning a three-part "Spring Seminar Series" to shine a light on several trends in Big Data and their impact on consumer privacy.[18] The series will focus on mobile device tracking in retails stores, the use of predictive scoring to help companies predict consumer behavior and shape how they market to particular consumers, and health apps that consumers increasingly use to manage and analyze their health data.

The FTC also will continue to aggressively enforce the FCRA, which sets forth procedures governing the use of data to make decisions about whether to give consumers credit, a job, or insurance.[19] The FCRA covers some of the practices of greatest concern when it comes to Big Data and remains a highly effective tool.

For example, the Commission recently obtained a $3.5 million penalty from Certegy, a company that advises merchants on whether to accept consumers' checks, based on their past financial history.[20] The complaint alleged that Certegy violated the FCRA by failing to have appropriate dispute procedures and failing to maintain the accuracy of the information it provided to merchants. This resulted in consumers – many of them elderly – being denied the ability to write checks and obtain essential goods and services.

We also sent warning letters to companies that were skirting too close to the FCRA line. Earlier this year, we conducted undercover test shops and issued warning letters to ten data

---

[17] FTC Workshop, *The Big Picture: Comprehensive Online Data Collection* (Dec. 6, 2012), *available at* http://www.ftc.gov/bcp/workshops/bigpicture/.

[18] FTC Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues* (Dec. 2, 2013), *available at* http://ftc.gov/opa/2013/12/springprivacy.shtm.

[19] 15 U.S.C. §§ 1681-1681x.

[20] *U.S. v. Certegy Check Servs., Inc.*, No. 1:13-cv-01247 (D.D.C. Aug. 15, 2013), *available at* http://www.ftc.gov/opa/2013/08/certegy.shtm.

brokers that appeared to be selling information for FCRA purposes without following the FCRA requirements.[21]

B. Mobile Technologies and Connected Devices

A second area of focus is mobile technologies and connected devices. Over the last few years, mobile technology has become one of the main privacy priorities for the Commission. On the policy front, the FTC has already issued several reports, including two reports showing the lack of mobile privacy disclosures about how kids apps are collecting and using data;[22] a report making recommendations on mobile privacy disclosures;[23] and a mobile payments report.[24] We hosted a workshop on mobile security earlier this year,[25] and expect to release a report in the next few months examining what we learned from that event.

We also have been active on the enforcement front in the mobile ecosystem. For example, earlier this year, the FTC also brought its first case against a mobile device manufacturer – HTC America.[26] The Commission alleged that HTC had basic security failures, such as the failure to provide guidance or training to engineering staff, test products and services, follow Android operating system security measures, and have appropriate procedures to keep abreast of security research. These failures caused numerous vulnerabilities, including the ability of unauthorized third parties to steal personal information, surreptitiously send text

---

[21] FTC Press Release, *FTC Warns Data Broker Operations of Possible Privacy Violations* (May 7, 2013), *available at* http://www.ftc.gov/opa/2013/05/databroker.shtm.

[22] FTC Staff Report, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012), *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf; FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

[23] FTC Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

[24] FTC Staff Report, *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments* (Mar. 2013), *available at* http://www.ftc.gov/os/2013/03/130306mobilereport.pdf.

[25] FTC Workshop, *Mobile Security: Potential Threats and Solutions* (June 4, 2013), *available at* http://www.ftc.gov/bcp/workshops/mobile-security/.

[26] *In the Matter of HTC America Inc.*, Docket No. C-4406 (June 25, 2013), *available at* http://ftc.gov/opa/2013/02/htc.shtm.

messages, and enable the device's mic to record the user's phone calls. As part of the order, HTC is required to undergo audits for 20 years and to implement security patches.

Our case against the social networking app Path, which I mentioned earlier, is another example of our heightened focus on law violations in the mobile space.

Of course, mobile is just the tip of the technology iceberg; beyond computers and smartphones, our world is getting more and more connected. Today, consumers can connect remotely to their refrigerators, bank accounts, thermostats, cars, and many other products and devices. Just last month, the FTC held a workshop on this phenomenon known as the "Internet of Things."[27] The workshop brought together academics, industry representatives, and consumer advocates to explore the security and privacy issues related to increased connectivity for consumers, including in areas such as smart homes, connected health and fitness devices, and connected cars.

The workshop explored the novel privacy and security issues raised by the Internet of Things, such as the difficulty of providing traditional notice and choice, and the fact that many players in the traditional consumer products space have less experience with privacy and security issues than their high-tech counterparts. Following the workshop, we are developing a report to summarize the findings and, where appropriate, set forth best practices for managing privacy and security with new interconnected devices. We are accepting public comments to inform our report until January 10.

In addition, the FTC recently announced its first "Internet of Things" case involving a video camera designed to allow consumers to monitor their homes remotely.[28] The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home

[27] FTC Workshop, *Internet of Things: Privacy & Security in a Connected World* (Nov. 19, 2013), *available at* http://www.ftc.gov/bcp/workshops/internet-of-things/.

security to baby monitoring, and claimed in numerous product descriptions that they were "secure." In fact, the cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address. This resulted in hackers posting 700 consumers' live feeds on the Internet. Under the FTC settlement, TRENDnet must maintain a reasonable security program, obtain outside audits, notify consumers about the security issues and the availability of the software update to correct them, and provide affected customers with free technical support for the next two years.

C. Protecting for Sensitive Data

A third area of focus is providing strong safeguards for sensitive data involving children, health information, and financial data. The FTC has long been concerned that this type of sensitive data warrants special protections.

When it comes to protecting children's privacy, this has been a big year at the FTC. In July, the final Children's Online Privacy Protection Act (COPPA) Rule went into effect. The Rule strengthens kids' privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under 13.[29]

The FTC updated the Rule to respond to collection practices made possible by new technology – namely, data-gathering tools like social media and mobile applications. To assist the business community with compliance, the Commission has sought to educate companies through a variety of means such as webinars, a compliance hotline, the business center blog, and other business guidance. Since going into effect, the FTC has been mindful of the impact of the Rule on businesses and has exercised prosecutorial discretion in enforcing the Rule, particularly with respect to small businesses that have attempted to comply in good faith in the early months

[28] *In the Matter of TRENDnet, Inc.*, Matter No. 122-3090 (Sept. 4, 2013), *available at* http://www.ftc.gov/opa/2013/09/trendnet.shtm.
[29] 16 C.F.R. Part 312.

after the Rule became final. However, as we approach six months since the effective date of the Rule, the FTC will begin to ramp up enforcement where needed to ensure compliance.

The Path case, which I mentioned earlier, illustrates the importance of kids' privacy and COPPA. Social networking app Path didn't just capture personal information from adults' address books; it also captured address book information from kids' devices, including full names, addresses, phone numbers, email addresses, dates of birth and other information, where available. In addition, Path enabled children to create personal journals and upload, store, and share photos, written "thoughts," their precise location, and the names of songs to which the child was listening. According to the complaint, Path did this without obtaining parental consent, in violation of COPPA.[30] The order required Path to pay $800,000 civil penalty, delete information from kids under 13, and prohibits Path from engaging in future violations.

In the area of health data, the FTC recently brought two cases of particular interest. In January, the Commission brought a case against Cbr, a leading cord blood bank, for failing to protect nearly 300,000 customers' personal information, including Social Security numbers, credit and debit card account numbers, and sensitive medical information.[31] The breach occurred when unencrypted back-up files and a laptop were stolen from a backpack left in an employee's car for several days. We also settled related allegations that Cbr failed to take sufficient measures to prevent, detect, and investigate unauthorized access to computer networks.

Most recently, the FTC filed a complaint against LabMD, a medical testing lab whose security we allege is unreasonable.[32] For example, the complaint alleges that LabMD's lax security enabled a high-level official to install a peer-to-peer (P2P) file-sharing application on a

---

[30] *U.S. v. Path, Inc.*, No. C-13-0448-JCS (N.D. Cal. Filed Jan. 31, 2013), *available at* http://www.ftc.gov/opa/2013/02/path.shtm.

[31] *In the Matter of Cbr Systems, Inc.*, Docket No. C-4400 (Apr. 29, 2013), *available at* http://www.ftc.gov/os/caselist/1123120/130503cbrcmpt.pdf.

[32] *In the Matter of LabMD, Inc.*, Docket No. 9357 (Aug. 28, 2013), *available at* http://www.ftc.gov/opa/2013/08/labmd.shtm.

work computer. As a result, highly sensitive information from over 9,000 consumers – including consumers' names, dates of birth, Social Security numbers, information relating to laboratory tests conducted, and health insurance policy numbers – was was found on a P2P network. In addition, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves. The LabMD litigation is ongoing.

Finally, financial privacy has been a priority for years. The FTC has brought many data security cases in which companies did not maintain reasonable security for consumers' financial information. Last June, the FTC filed a complaint against Wyndham Hotels for failure to protect consumers' personal information, resulting in three data breaches in less than two years.[33] According to the FTC's complaint, Wyndham and its subsidiaries failed to take reasonable and basic security measures, such as using complex user IDs and passwords and deploying firewalls and network segmentation between the hotels and the corporate network. In addition, Wyndham allegedly permitted improper software configurations that resulted in the storage of sensitive payment card information in clear readable text.

The complaint alleges that these failures resulted in fraudulent charges on consumers' accounts, millions of dollars in fraud loss, and the export of hundreds of thousands of consumers' account information to an Internet domain address registered in Russia. This case, like LabMD, is currently in active litigation. However, let me stress that the standard here – and in all our data security cases – is *reasonable* security, not perfection. We only bring cases where, we allege, a company has clearly fallen below that standard.

IV. Legislation

[33] *FTC v. Wyndham Worldwide Corp. et al.*, No. 2:13-cv-01887-ES-SCM (D.N.J. Mar. 25, 2013), *available at* http://www.ftc.gov/opa/2012/06/wyndham.shtm.

Lastly, I want to briefly address the topic of privacy and security legislation. Some of us at the FTC support omnibus legislation – for both privacy and data security – because it would create clear and consistent standards for everyone; even the playing field (and, indeed, provide an advantage) for legitimate businesses; make non-consumer facing businesses like data brokers accountable; and provide greater clarity about the U.S. commitment to privacy as we deal with our international partners. As I've watched developments in privacy since the mid- to late- 90s, the world of consumer data has only gotten more complicated. There seem to be obvious benefits to boiling privacy and security down to their basics and making sure everyone at least gets those right.

I know that privacy legislation seems like a far-off goal right now, but data security does not. People on many sides of the issue have supported data security legislation for years. Although there's a fair amount of controversy about privacy, no one seems to think that making consumer data vulnerable to identity theft is a good thing – except the identity thieves. I urge everyone in this room to think about whether 2014 could finally be the year we get data security legislation.

V. Conclusion

In closing, I think it's safe to promise you that 2014 will be just as busy as 2013 and that we'll be focusing on big data, connected devices, and protecting sensitive data. Across all of our areas of focus, we will keep reminding companies to implement the three privacy principles we set out in our 2012 Privacy Report – Privacy-By-Design, Transparency, and Simplified Choice. Finally, we will continue to support robust self-regulation. We have seen some promising developments on this front – including the efforts undertaken by the Better Business

Bureau enforce the online advertising principles of the Digital Advertising Alliance (DAA)[34] – and we want those efforts to continue.

Best wishes for the upcoming year. I am happy to take questions.

[34] *See, e.g.*, Better Business Bureau Press Release, *Accountability Program Instructs Advertiser, Agency and Platform to Work Together to Deliver AdChoices Icon* (Nov. 20, 2013), *available at* http://www.bbb.org/council/migration/bbb-news-releases/2013/11/accountability-program-instructs-advertiser-agency-and-platform-to-work-together-to-deliver-adchoices-icon/; Better Business Bureau Press Release, *Accountability Program Decisions Throw Spotlight on Website Operators' Compliance* (Nov. 18, 2013), *available at* http://www.bbb.org/council/migration/bbb-news-releases/2013/11/accountability-program-decisions-throw-spotlight-on-website-operators-compliance/.