Cravath/NYC Bar Institute for Corporate Counsel
New York City, NY
December 10, 2014
Remarks of Commissioner Terrell McSweeny[1]

Hello, I am delighted to be here. Thanks to Christine Varney and Cravath for the invitation.

My arrival at the FTC earlier this year coincided with a very special time for the agency. One hundred years ago, President Woodrow Wilson signed legislation creating the Federal Trade Commission. We've spent a good bit of time this year both celebrating and, importantly, reflecting on the FTC's history and accomplishments. Many things have changed since 1914, of course. The FTC started out as an agency focused on "trust-busting" and is now at the forefront of competition and consumer protection issues that Woodrow Wilson likely couldn't even imagine in his day. What would he have made of apps, smartphones and social networks?

While Wilson and the architects of the FTC couldn't have anticipated all the innovations of our highly connected 21st century economy, they did appreciate that the FTC's competition and consumer protection mission would need to evolve along with the economy.

That's why they did two things when they created the Commission: (1) they gave the commission tools to inform its mission and develop expertise by studying markets and business practices; and (2) they gave the commission enforcement authority flexible enough to keep pace with innovation.[2] What I'm going to talk about today is how the FTC is using these long-standing authorities to protect 21st century consumers.

FTC@100: "Federal Technology Commission"

The modern Federal Trade Commission has sometimes been called the "Federal Technology Commission" because over the last decade it has emerged as the preeminent consumer privacy and data security enforcement agency. The Commission's recent consumer protection cases involve the application of old, well-established consumer protection law to new, cutting-edge technologies.

For example, this year the Commission brought two cases against mobile phone carriers seeking redress for unauthorized third party charges on mobile phone bills that were ostensibly for monthly subscriptions to receive information such as horoscopes or celebrity gossip.[3]

---

[1] The views expressed in this speech are my own and do not necessarily reflect those of the Commission or any other Commissioner.

[2] *See* 15 U.S.C. § 45(a).

[3] *See e.g.* Compl., *FTC v. AT&T Mobility, LLC*, No. 1:14-mi-99999-UNA (N.D. Ga. filed Oct. 8, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141008attcmpt1.pdf; Compl., *FTC v. T-Mobile USA, Inc.*, No.

The Commission has been protecting consumers from this practice – sometimes called cramming – for more than 15 years. Starting in the late 1990s, the FTC targeted cramming on landlines – cracking down on scammers and studying the impact of the practice on consumers.[4] Not surprisingly, as we adopted mobile phones, cramming scams moved from the analog to the mobile world. So did the FTC by bringing cases not only against the fraudsters who implement these scams – but also, this year, against carriers.

In these cases, the Commission alleged that the carriers deceptively described unauthorized cramming charges on phone bills in a manner that made it difficult for consumers to discover them and continued to charge consumers even after they became aware of telltale signs that charges were unauthorized.[5] These actions reinforce that basic consumer protection principles apply in the mobile environment – just as they do in the brick-and-mortar world.

The FTC has applied the same principles in its in-app purchase cases – reinforcing that consumers have the same protections on mobile as they do in traditional retail transactions. In the last year, the Commission settled with Apple and Google and is litigating against Amazon – for billing parents, without their authorization, for purchases made by children in apps directed to kids. Some parents were billed hundreds, or even thousands, of dollars when their children bought things like virtual coins or upgraded virtual racecars. Apple and Google have agreed to refund a total of more than $50 million dollars and institute new measures to insure that parents can better control in-app purchases by children.[6]

To be clear, there is nothing wrong with a mobile app providing the capability to make purchases with real money. The problem is when children are able to make purchases without getting their parents' password or permission and when parents have no recourse to dispute unauthorized virtual spending sprees by their children. Again – in these cases, the FTC is reinforcing well-established consumer protection law that you cannot charge consumers without their express, informed consent.

2:14-cv-00967 (W.D. Wa. filed July 1, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140701tmobilecmpt.pdf.

[4] *See e.g.*, *FTC v. Inc21.com Corp.*, 745 F. Supp. 2d 975 (N.D. Cal. 2010), *aff'd*, 2012 WL 1065543 (9th Cir. Mar. 30, 2012); *FTC v. Hold Billing Servs., Ltd.*, No. 98-cv-00629-FB (W.D. Tex.) (contempt motion filed March 28, 2012); *FTC v. Nationwide Connections, Inc.*, No. 06-80180 (S.D. Fla. Sept. 18, 2008) (stipulated final order); *FTC v. Websource Media, LLC*, No. H-06-1980 (S.D. Tex. July 17, 2007) (stipulated final order); *FTC v. Epixtar Corp.*, No. 03-8511 (S.D.N.Y. Nov. 29, 2006) (stipulated final order); *FTC v. Mercury Mktg. of Del., Inc.*, No. 00-3281, 2004 WL 2677177 (E.D. Pa. Nov. 22, 2004); *FTC v. 800 Connect, Inc.*, No. 03-CIV-60150 (S.D. Fla. Feb. 4, 2003) (stipulated final order); *FTC v. Access Resource Servs., Inc.*, No. 02-CIV-60226 (S.D. Fla. Nov. 4, 2002) (stipulated final order); *FTC v.Cyberspace.com, LLC*, No. C00-1806L, 2002 WL 32060289 (W.D. Wash. July 10, 2002), *aff'd*, 453 F.3d 1196 (9th Cir. 2006).

[5] *See e.g.* Compl., *FTC v. AT&T Mobility, LLC*, No. 1:14-mi-99999-UNA (N.D. Ga. filed Oct. 8, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141008attcmpt1.pdf; Compl., *FTC v. T-Mobile USA, Inc.*, No. 2:14-cv-00967 (W.D. Wa. filed July 1, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140701tmobilecmpt.pdf.

[6] *See* Press Release, In the matter of Apple, Inc., Dkt. C-4444 (Mar. 27, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million; Press Release, In the matter of Google, Inc., Dkt. C-4499 (Dec. 5, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-case-about-google-billing-kids-app.

Another recent case, which the Commission announced two weeks ago, concerns the use of social media as a platform for advertising. In this case, the Commission alleged that an advertising agency working on behalf of Sony to promote a new gaming device had its employees post messages to Twitter endorsing the Sony product – without disclosing their connection to Sony.[7]

Privacy & Security

The FTC's prohibition against deceptive acts and practices also applies to promises companies make about their privacy practices.

For example, this year the FTC brought a case against Snapchat – which grew from hosting 25 images a day to becoming one of the top content and social media sites on the Web, with nearly 500 million pictures and videos uploaded each day partly because of its claim that once viewed by a recipient, the content disappeared forever. The Commission charged that those representations were untrue.[8] By simply connecting a device to a computer, or downloading a third party app, or even taking a screen-grab, users could create a permanent record of the image despite Snapchat's claims. There appears to be growing competition on privacy among apps, services and platforms, which is a very encouraging development. The FTC will continue to look carefully at marketing claims about privacy to insure they are accurate.

Some of the FTC's privacy cases also involve data security issues. The failure to employ reasonable security measures to protect personal information can violate the FTC Act's prohibition against unfair acts or practices, even if the failure does not violate a promise made by a firm. For instance, earlier this year we brought a case against GMR Transcription Services. GMR, a medical transcription company, hired contractors to transcribe files. The contractors downloaded the files, transcribed them, and then uploaded them once completed. But the Commission alleged that because of inadequate network security, the files became indexed by various internet search engines and appeared online for the whole world to see.[9] Since they were medical files, very sensitive information was exposed.

As consumers, we are increasingly using connected devices in our homes – bringing the so called "Internet of Things" into our most private spaces. While these innovations enable wonderful new products – they can present new risks when security and privacy are not part of the product design. The FTC is studying these issues and also bringing enforcement actions in situations where the sanctity of the home is invaded without permission, or exposed because of lax security.

---

[7] *See* Compl., In the matter of Sony Computer Entertainment America LLC, FTC File No. 122-3252 (Nov. 24, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141125sonycmpt.pdf.

[8] *See* Compl., In the matter of Snapchat, Inc., FTC File No. 132-3078 (May 8, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf.

[9] *See* Compl., In the matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekant Srivastava, Dkt. C-4482 (Aug. 21, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf.

Designerware and TRENDNet are recent examples. Designerware provided software to rent-to-own companies to place on computers. The software had a "Detective Mode" that could log keystrokes, take screen shots, and turn on webcams – all without the knowledge of the computer user.[10] TRENDNet marketed home security and baby monitoring cameras, claiming they were secure. However, the cameras were not secure and had faulty software that left them open to online viewing by unauthorized users.[11] All that was needed was the Internet address of the camera, and viewers around the world could watch what the camera recorded – babies asleep in their cribs, families at dinner around their kitchen table.

These cases are privacy cases – and, also, fundamentally security cases. The FTC has brought more than 50 data security cases since 2002.[12] These cases have helped to establish best practices for data security in the commercial sector. But each new revelation of large-scale breaches show that more must be done. The problem was front and center this year with the news of multiple high-profile breaches. Indeed, 60 Minutes called 2014 "The Year of the Data Breach."[13] The American public is concerned. A recent Gallup poll revealed that 70% of Americans are worried about the security of their data and would support comprehensive federal data breach legislation.[14]

All five FTC Commissioners, Republican and Democrat, have called on Congress to pass national legislation to establish baseline data security requirements and establish procedures for companies and other institutions to follow in cases of data breach, rather than applying a patchwork of 47 different state laws.[15]

In the absence of legislation, however, the President announced the new "Buy Secure" initiative earlier this year. The initiative will give the FTC new tools to report and combat identity theft by expanding the resources of our IdentityTheft.Gov web site and by streamlining

---

[10] *See* Compl., In the matter of DesignerWare, LLC, Timothy Kelly, and Ronald P. Koller, Dkt. C-4390 (Apr. 15, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf.

[11] *See* Compl., In the matter of TRENDnet, Inc., Dkt. C-4426 (Feb. 7, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[12] Fed. Trade Comm'n, Federal Trade Commission 2014 Privacy and Data Security Update at 3 (June 2014), *available at* http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

[13] Bill Whitaker, What Happens When You Swipe Your Card?, CBS News 60 Minutes, Nov. 30, 2014, *Transcript available at* http://www.cbsnews.com/news/swiping-your-credit-card-and-hacking-and-cybercrime/.

[14] *See e.g.* Rebecca Rifkin, Hacking Tops List of Crimes Americans Worry About Most, Gallup, Oct. 27, 2014, *available at* http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx.

[15] *See, e.g.*, Prepared Statement of the Federal Trade Commission, "Protecting Personal Consumer Information from Cyber Attacks and Data Breaches," Before the Senate Committee on Commerce, Science, and Transportation, 113th Cong., Mar. 26, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf; Prepared Statement of the Federal Trade Commission, "Data Breach on the Rise: Protecting Personal Information from Harm," Before the Senate Committee on Homeland Security and Governmental Affairs, 113th Cong., Apr. 2, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf.

the credit and identity repair process for consumers.[16] The FTC recognizes that tens of thousands of people are victims of ID theft each year. The Commission receives more consumer complaints involving ID theft than any other area – 290,000 over the last year, nearly 6,000 complaints a week.[17]

The FTC is constantly examining new issues in technology - including through a series of workshops, roundtables, and reports this year. At a recent workshop on Big Data, the FTC explored the legal and policy ramifications surrounding how large data sets could, in effect, create the redlining and discrimination that our traditional legal framework was established to prevent.[18] The Commission is considering questions such as: Can unregulated algorithms foreclose job and credit opportunities for some people? What choices should consumers have about when location data and other information is passively gathered about them?

The FTC is also examining the impact of the exponentially growing world of the Internet of Things. By the end of next year, we expect there to be 25 billion connected devices.[19] This number should double by 2020[20] – when, according to the Alliance of Automobile Manufacturers, more than 90% of cars will be connected to the Internet,[21] and 15 quintillion bytes of information will be generated by Internet connected things each month.[22] To put it into perspective, the Internet will soon be generating more data *in a month* than all of humanity did in all of the years before the Internet.

The use of embedded sensors to gather and transmit data between devices and into the cloud is creating new issues of consumer notice and consent. It also raises the stakes around how this information is secured.

At the FTC, we recognize that there is no such thing as perfect data security. Reasonableness of security procedures is our touchstone and companies should make every best effort to secure their networks and ensure the data they collect is protected. The FTC has

---

[16] White House, FACT SHEET: Safeguarding Consumers' Financial Security (Oct. 17, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/10/17/fact-sheet-safeguarding-consumers-financial-security.

[17] Fed. Trade Comm'n, Consumer Sentinel Network Data Book for January – December 2013 at 6 (Feb. 2014), *available at* http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf.

[18] *See* Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion?, *available at* http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion

[19] Cisco Internet Business Solutions Group, The Internet of Things How the Next Evolution of the Internet Is Changing Everything at 3 (Apr. 2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[20] *Id.*

[21] Telefonica, Connected Car Industry Report 2013 at 9 (2013), *available at* http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.

[22] Cisco, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018 at 3 (Feb. 5, 2014), *available at* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

provided a process-based framework for businesses and consumers on how to assess data security risks.[23]

One way that private companies may defend against cyber attacks is by sharing technical cyber threat information with one another – such as incident or threat reports, threat signatures, indicators, and alerts. Some private-to-private threat information sharing is taking place today through both informal and formal exchanges and agreements. The sharing of information in this context can improve efficiency and help keep our information networks and resources secure.

Understandably, however, companies may be reluctant to share this information with each other – particularly if they are competitors – out of fear that such conduct would run afoul of the antitrust laws.

In response to this concern, in April, the Department of Justice and the FTC set forth an antitrust policy statement on the sharing of cybersecurity information.[24] The policy statement confirms that antitrust should not be a roadblock to legitimate information sharing about cyber threats and attacks. Cyber threat information tends to be very technical in nature. This is very different from the sharing of competitively sensitive information about pricing, costs, output, or other company-specific plans. The policy statement also recognizes that information-sharing arrangements are less likely to facilitate collusion on competitively sensitive data if companies implement safeguards designed to prevent such disclosure.

Issues of data security and privacy are increasingly challenging internationally. Cross-border data flows are not just important for the ease of operations within a company – they underpin the very essence of a "World Wide Web." The FTC is the enforcement agency within our government that oversees the implementation of the U.S.-EU Safe Harbor Agreement, which provides a method for U.S. companies to transfer personal data lawfully from the EU to the U.S. Companies promise to follow the Safe Harbor privacy principles and the FTC enforces these promises. The FTC is working to ensure that Safe Harbor is maintained so that companies can continue to process information and data between operations located in Europe and the United States.[25]

---

[23] *See e.g.* Fed. Trade Comm'n, Protecting Personal Information: A Guide for Business (Nov. 2011), *available at* http://www.business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf.

[24] Dept. of Justice and Fed. Trade Comm'n: Antitrust Policy Statement on Sharing of Cybersecurity Policy Information, *available at* http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.

[25] *See e.g.* Fed. Trade Comm'n, Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework (Nov. 12, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf*; See generally* Fed. Trade Comm'n, Safe Harbor Program, *available at* http://business.ftc.gov/content/safe-harbor-program.

Policy Questions At the Intersection of Technology, IP and Antitrust

Another area in which the FTC is using well-established authorities to address troubling new conduct is the deceptive use of demand letters, and other potentially abusive tactics, by patent assertion entities (PAEs). As most of you know, PAEs are firms that buy patents and monetize them by asserting them against practicing entities. Discussion over the last two years has centered around the degree to which PAEs impact innovation and completion. On the one hand, critics argue PAEs are causing companies and innovators to put more resources into patent litigation than research and development. On the other hand, proponents argue that PAEs develop a valuable secondary market for patents, enabling inventors to recoup costs and fund new projects.

However, there is growing consensus that PAEs that send out thousands of demand letters in an effort to extract payments from users of a product are behaving deceptively. Earlier this year, the FTC brought action against MPHJ, a patent assertion entity, for sending out letters to 9,000 different small businesses threatening legal action.[26] The letters alleged that the companies were illegally sending emails of scanned documents from a networked copier – something I think most of us have done – without paying a licensing fee to do so. In its letters, MPHJ claimed that "many other businesses" have paid for a license, and that failure to pay would result in legal action. Neither of those claims was true, and the deceptive letters led to FTC action.

The Commission also is examining competition policy issues as they relate to PAEs. We hosted a workshop with the Department of Justice on the subject of patent assertion entities in 2012, and received approval this summer to conduct a 6(b) study on PAEs.[27] We recently issued information requests to respondents in connection with that study, and we hope to learn how PAEs do business and how they affect innovation and competition. The FTC intends to publish a descriptive report that will allow industry participants, policymakers, and academics to gain a better understanding of all aspects of the PAE business model.

I also believe that the Commission should continue to pursue enforcement efforts against PAEs, where appropriate. Moreover, I am hopeful that progress will be made on patent reform in the new Congress.

PAEs are among the number of issues the FTC is focused that arise at the intersection of intellectual property and antitrust. The FTC has been – and will continue to be – very focused on the licensing practices surrounding FRAND-encumbered standards essential practices. And in the pharmaceutical industry, the Commission is continuing its efforts to stop reverse payment settlements (or "pay-for-delay" agreements) after the Supreme Court's ruling in our case against pharmaceutical company Actavis last year. The FTC has been studying the effect of reverse payment settlements – and enforcing against them where appropriate – for over 15 years. The

[26] *See* Compl., In the matter of MPHJ Technology Investments, LLC, FTC File No. 142-3003 (Nov. 6, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141106mphjcmpt.pdf.

[27] *See generally* Patent Assertion Entities (PAE) Study, *available at* http://www.ftc.gov/policy/studies/patent-assertion-entities-pae-study.

Supreme Court's *Actavis* decision was significant in confirming the harm to competition from reverse payment agreements.[28] But the Supreme Court left it to the lower courts to structure the rule-of-reason analysis.

The Commission has three ongoing reverse payment settlement litigations: *Actavis*, now on remand to the district court, *Cephalon*, also pending in district court, and a case against AbbVie, Besins, and Teva that was filed in September. In the most recent case, the Commission alleges that AbbVie and its partner Besins filed sham patent litigation suits against potential generic competitors in order to delay introduction of lower-priced versions of AbbVie's blockbuster drug AndroGel.[29] The reverse payment agreement we allege is not cash – but that AbbVie paid Teva in the form of an authorized generic deal on another drug (TriCor).

The Commission also looks to shape the contours of the law through amicus opportunities. For example, earlier this year, the FTC filed an amicus brief in the Lamictal direct purchaser litigation pending before the Third Circuit, arguing that "no authorized generic commitments" present similar concerns to those identified by the Supreme Court in *Actavis*.[30] I expect that the Commission will continue to be an integral player in bringing cases, where appropriate, post-*Actavis*.

Conclusion

As you can tell, our centennial year has been a busy one. In the interest of time, I did not discuss our portfolio of merger review and enforcement efforts. However, as many of you are personally well aware, merger activity has been very active this year. According to Thomson Reuters – and as reported in the New York Times, about $1.5 trillion in transactions targeting American companies were announced this year – the most since 2000.[31] The FTC will continue its careful evaluation of mergers and acquisitions.

I expect the FTC @101 will continue to use the authorities and tools Congress invested it with 100 years ago to protect consumers and competition.

Thanks again for having me here today.

---

[28] *FTC v. Actavis, Inc.*, 133 S. Ct. 2223 (2013).

[29] Compl., *FTC v. AbbVie, Inc.*, No. 14-CV-5151 (E.D. Pa. filed Sept. 8, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140908abbviecmpt1.pdf.

[30] Br. of Fed. Trade Comm'n as *Amicus Curiae* in Supp. of Pl.-Appellants, *King Drug Co. of Florence, Inc. v. SmithKlineBeecham Corp.*, No. 14-1243 (3d Cir. filed Apr. 28, 2014), *available at* http://www.ftc.gov/system/files/documents/amicus_briefs/re-lamictal-direct-purchaser-antitrust-litigation/140428lamictalbrief.pdf.

[31] David Gelles, Mega-Mergers Popular Again on Wall Street, NY Times, Nov. 17, 2014, *available at* http://dealbook.nytimes.com/2014/11/17/mega-mergers-popular-again-on-wall-street/.