Net Neutrality and Transatlantic Privacy
Keynote Address Before Hogan Lovells Winnik International
Telecoms & Internet Forum
December 16, 2015

Thank you, Ari, for your kind introduction. It is a pleasure to wrap up this most eventful year in Internet legal developments here at the Winnik Forum. When Ari invited me to speak with you today, I thought two topics all of you might be interested in hearing about were the FTC-FCC relationship in the wake of the Open Internet Order and transatlantic privacy in the wake of the European Court of Justice's Safe Harbor decision. When I asked him which one he would like me to address, he said, "Yes." And far be it from me to be the Winnik Forum's Scrooge by denying Ari his holiday wish!

Reclassifying Privacy Protections Under the Open Internet Order

So let me jump right in by focusing first on the Open Internet Order, its implications for the FTC, and its significance for privacy. The Open Internet Order, which the FCC issued in February of this year, reclassified broadband ISPs as common carriers that are subject to Title II of the Communications Act.[1] I support the main goal behind the Open Internet Order, which is to prevent the blocking or degradation of sites and services that consumers want to reach. I believe that the Open Internet Order will help to achieve these goals.

The main purpose of the Open Internet Order is to deal with the issue of net neutrality, but it also holds major implications for privacy and data security. I welcome an expanded role for the FCC in enforcing consumer privacy protections. The Open Internet Order moves the FTC out of enforcement in a narrow but significant band of commercial activity on the Internet, but it is important to note how limited the real world impact of this restriction on the FTC's jurisdiction will be. It only affects ISPs in their capacity as common carriers. Consumer privacy enforcement, however, continues to present a target-rich environment, and even with the Open Internet Order, the FTC keeps its place as the nation's leading consumer protection and privacy agency. Our consumer protection authority extends to the apps, edge services, ad networks, advertisers, publishers, data brokers, analytics firms, and the many other actors whose data practices are part of the delivery of valuable services to consumers but also, in some instances, raise privacy and data security concerns. And, of course, the FTC's jurisdiction extends far beyond that – we have authority over any unfair or deceptive acts affecting commerce, unless specifically carved out from the FTC's jurisdiction.[2]

Thus, I do not share the concerns of those who believe that the FTC has been dramatically shoved aside. A better option, of course, would be to remove the common carrier exemption to Section 5 of the FTC Act – a change that the FTC has been recommending to

[1] FCC, In the Matter of Protecting and Promoting the Open Internet, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order (Mar. 12, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf ["Open Internet Order"].

[2] *See* 15 U.S.C. § 45(a).

Congress for the past decade.[3] The exemption is an artifact. It dates from a time when the horse-and-buggy ruled the streets and the Interstate Commerce Commission was a force to be reckoned with. Today, however, the exemption threatens to leave a gap in the nation's consumer protection laws.

And I believe the two agencies would work well to ensure our enforcement efforts are efficient, and that we don't "double team" potential targets. Where the FTC and FCC overlap in other enforcement areas, we have long had a successful working relationship. The FTC and FCC have cooperated since 2003 under a memorandum of understanding (MOU) that applies to telemarketing enforcement issues.[4] And last month, the two agencies announced an additional MOU that covers other areas of consumer protection enforcement that we have in common.[5] This new MOU recognizes the agencies' respective areas of expertise, expresses a desire to avoid conflicting or duplicative actions, and outlines specific steps that the agencies will take to remain in sync. An MOU of similar breadth is in place between the FTC and the Consumer Financial Protection Bureau,[6] and it has worked well in terms of formalizing cooperation and providing clarity to stakeholders in the private sector.

The rationale for creating dual FTC-FCC jurisdiction over common carriers is strong. The FTC and FCC bring different kinds of expertise and have complementary authority that, when brought together, could form a highly effective consumer protection regime. The FTC has the authority to obtain restitution for consumers when they lose money as a result of deceptive or unfair practices. The FCC does not have this authority. We also have vast experience with developing orders that stop bad conduct, and with monitoring those orders to make sure they stick. The FCC, on the other hand, has broad civil penalty authority, which deters companies under its jurisdiction from repeating misbehavior, as well as deterring other players in those sectors that may be considering similar conduct. It also has the authority to issue privacy rules through notice-and-comment rulemaking – something that the FTC cannot do.

Looking beyond the FTC-FCC relationship, I see an important opportunity under the Open Internet Order for a vigorous discussion about privacy. The Open Internet Order puts ISPs

---

[3] *See* Prepared Statement of the Federal Trade Commission on FTC Jurisdiction over Broadband Internet Access Services, Presented before the Committee on the Judiciary, United States Senate (June 14, 2006), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-ftc-jurisdiction-over-broadband-internet-access-services/p052103commissiontestimonyrebroadbandinternetaccessservices06142006senate.pdf.

[4] *See* FCC – FTC Memorandum of Understanding on Telemarketing Enforcement, reproduced as an appendix in FTC, Annual Report to Congress for FY 2003 and 2004 Pursuant to the Do Not Call Implementation Act on Implementation of the Do Not Call Registry (Sept. 2005), available at https://www.ftc.gov/sites/default/files/documents/reports/national-do-not-call-registry-annual-report-congress-fy-2003-and-fy-2004-pursuant-do-not-call/051004dncfy0304.pdf.

[5] Memorandum of Understanding on Consumer Protection Between the Federal Trade Commission and the Federal Communications Commission Nov. 2015), *available at* https://www.ftc.gov/policy/cooperation-agreements/memorandum-understanding-consumer-protection-between-federal-trade.

[6] *See* Memorandum of Understanding Between the Consumer Financial Protection Bureau and the Federal Trade Commission (Mar. 2015), *available at* https://www.ftc.gov/policy/cooperation-agreements/ftc-cfpb-interagency-cooperation-agreement.

under section 222 of the Communications Act, including the FCC's authority to write rules under this law. The FCC has indicated that it will develop privacy rules in the coming months.

Let me also be clear about where I stand on this issue. Because ISPs play a different role and face a much different set of consumer expectations than edge services, I believe we should also consider privacy rules tailored for them.

Recognizing ISPs' Special Role in Consumers' Lives

There are three guiding principles that I believe the FCC should consider in the development of a privacy rule for ISPs. The first is that ISPs play a central and unique role in most consumers' lives. They provide the gateways through much of our online lives flow. Consider what happens when you go through a typical day. Throughout the night, a connected onesie has been sending information about your newborn's heart and breathing rate to an app installed on your smartphone. You wake up and, before your eyes are really open, start checking not only the overnight stats about your newborn, but also your email, the weather, and the news through your smartphone. You can also use your smartphone to adjust the heat and start your coffee maker, and determine how much energy your household used overnight. Meanwhile, your kids use their phones to do last-minute research for school and chat on the latest social networks with their friends. And in the evening, the streams from your game console and video streaming services dwindle, one by one, as members of your household retire for the night.

Think of the deeply personal portrait that you could develop from this information, which is "just metadata" – the IP addresses to which you connect and the time at which connections occur, it can get an intimate portrait of your interests, daily rhythms, habits – as well as those of all members of your household. The ISP can detect whether you're visiting health-related websites, for example, and even whether a health-related question might be keeping you up at night. The ISP can infer the presence of your kids in a household. And as the Internet of Things becomes more deeply embedded in consumers' lives – experts predict that the number of connected devices will double in five years to 50 billion[7] – data from these connected devices, that reveals your behavior directly or through inference, will become even more detailed and voluminous.

The FTC recognized in its 2012 Privacy Report that broadband providers' status as "a major gateway to the Internet" gives them "access to vast amounts of unencrypted data" that they could use to "develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible" to consumers.[8] Moreover, it may be very

[7] DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[8] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 56 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (noting that ISPs have "access to vast amounts of unencrypted data that their users send or receive over the ISP's network" and thus are "in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible") [2012 PRIVACY REPORT].

difficult for consumers to switch away from their broadband providers if they dislike the provider's data practices, because of the limited choice of high-speed providers that many consumers have. Finally, consumers pay for their broadband service – and pay a lot. The implicit bargain that many view as the basis for "no-cost" consumer services on the Internet – acceptance of targeted advertising in exchange for access to such services – makes much less sense when you are paying 50 dollars or more each month.[9]

Addressing Personal Data Use and Disclosure

The second guiding principle for a privacy rule that applies to ISPs is that it should address personal data *disclosure* and *use*. The sensitive information that ISPs can collect or infer about consumers could be used in two ways for marketing. First, an ISP it could determine which of its customers seems to be interested in some topic or area, such as health-related issues. The ISP could then provide lists of these consumers to edge services, publishers, and marketers. This is a form of disclosure; the ISP informs third parties which of its customers are interested in health issues. Alternatively, the ISP could *use* this information itself to target ads. Such an arrangement may be part of the future that some broadband providers are envisioning for themselves.[10]

Is one approach more privacy-protective than the other? Both of the scenarios that I outlined involve activities that are outside of what many consumers expect of their ISPs. The FTC has long expressed concerns about the ability of services that interact directly with consumers, as well as those that are hidden behind the scenes, such as ad networks and data brokers, to track and profile consumers. Disclosures of a consumer's interest in certain health conditions, her financial status, or her reading and music listening habits for that matter, might be deeply embarrassing. These concerns apply with greater force to broadband providers. The ISP that provides the consumer access to the Internet has all of her web activities at hand. If an ISP were to use this information for the separate purpose of developing marketing profiles or helping marketers to track consumers across different sites and services, I believe that use would be quite out of context of the understood relationship that the consumer has with the ISP, and consequently just as potentially harmful to consumer privacy.

Fortunately, section 222 addresses both disclosure and use.[11] It would be consistent with the Open Internet Order's animating idea – keeping broadband providers focused on delivering the service that consumers expect – to apply both concepts to a new rule under section 222.

---

[9] *See, e.g.*, Open Technology Institute at New America, The Cost of Connectivity 2014 (Oct. 30, 2014), *available at* https://www.newamerica.org/oti/the-cost-of-connectivity-2014/ (indicating that $50/month is a typical price for residential broadband service in the U.S.).

[10] *See, e.g.*, Mike Shields and Thoma Gyrta, *Verizon Agrees to Buy AOL for $4.4 Billion*, WALL ST. J. (May 12, 2015), *available at* http://www.wsj.com/articles/verizon-to-buy-aol-for-4-4-billion-1431428458 (discussing relationship of AOL's online advertising technology and Verizon's residential broadband services).

[11] *See, e.g.*, 47 U.S.C. § 222(c)(1) ("Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.").

Security is Paramount

Finally, a rule under section 222 should address data security. Of course, ISPs already have strong incentives to keep their networks up and running. Nothing provokes calls from customers more quickly than a network outage, whether it is the result of a backhoe cutting a fiber optic cable or a denial of service attack on a network gateway slowing traffic to a crawl. In this sense, broadband provider network security is already a critical aspect of ensuring that the service delivered to consumers is available and reliable.

The more novel security issues in the broadband context come from the data about consumers that ISPs have. ISPs possess data that could expose much of the same information whose unauthorized disclosure the FTC has found to be harmful, including health and financial information. Maintaining the privacy of this information is largely hopeless without ensuring that this data is kept appropriately secure. Like other companies that maintain huge amounts of sensitive data about their customers, ISPs could become an attractive target for attackers, and the risk to consumers increases as the amount of data that ISPs store increases. As a result, ISPs should also be held accountable for maintaining appropriate security for consumers' data. I expect that there will be a lot more discussion about whether and to what extent to make data security part of any further policy that flows from the Open Internet Order. At this point, I simply want to make sure that the fundamental connection between privacy and data security is not lost.

Transatlantic Privacy

Now let me turn to transatlantic privacy issues, where the past few months have revolved around similarities and differences between U.S. and European approaches to privacy. The most significant development in this regard, of course, is the *Schrems* decision, in which the ECJ invalidated the European Commission's decision regarding the adequacy of the U.S.-EU Safe Harbor framework.[12] Although *Schrems* has been highly disruptive for the thousands of businesses that were members of Safe Harbor and for other reasons I'll discuss in a minute, the decision was helpful in one way. It crystallized what has been clear – or should have been clear – for a long time about commercial privacy in Europe: it is a fundamental right that Europeans and their Court take very seriously.

Now, the job of U.S. and European negotiators is to figure out how to make it clear that a general, transparent, enforceable transatlantic data protection framework can comport with these fundamental rights. I believe that it can.

The *Schrems* decision focuses on two deficiencies European Commission's Safe Harbor decision. First, the Court worried about the Commission's silence on existing safeguards in the U.S. with respect to government access to personal data for purposes of national security surveillance.[13] Second, the Court was concerned about the lack of any information about the

[12] Schrems v. Data Protection Comm'r, CJEU Case C-362/14 (Oct. 6, 2015), *available at* http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre=.

[13] *See Schrems*, *supra* note 12, at ¶¶ 89-91.

availability of redress for individuals with respect to government access to personal data. The Court further held that, before there can be a finding of "adequacy" of the laws of another country or a data transfer mechanism, the European Commission must demonstrate that the privacy laws and other protections are "essentially equivalent" to those found in the European legal order.

I believe that this "essentially equivalent" standard requires a comparison between laws as they actually exist in the United States and at the EU and Member State levels, rather than a comparison of the United States' laws (or the laws of any third country) to European legal ideals as enshrined in the Charter of Fundamental Rights. Whether the ECJ agrees with me remains to be seen. But, in the meantime, I am engaging extensively with officials from the European Commission and Member State DPAs to explain the many ways that the United States protects personal data through a combination of constitutional, statutory, and administrative measures. This constant effort is necessary to improve the understanding of U.S. privacy protections in Europe, and my hope is that it provides a foundation for the honest conversation about privacy that needs to take place between Europe and the U.S.

In the short term, this honest conversation is focusing on putting in place a new transatlantic data transfer framework. Although advocates and DPAs haled the *Schrems* decision as a victory for the fundamental right of privacy, some of the losses are now becoming apparent. The first loss is transparency. When a company joined Safe Harbor, consumers knew it, advocates knew it, and the entire enforcement community knew it. The principles and operating procedures for Safe Harbor were also well known and uniform.[14] The same cannot be said for other data transfer mechanisms, such as binding corporate rules and model contractual clauses.

The second loss is FTC enforcement. Simply put, the absence of Safe Harbor may limit the FTC's ability to take action against companies if they misrepresent how they follow European privacy standards. And, in the absence of Safe Harbor, there is little reason for companies to make those representations in the first place. Before *Schrems*, The FTC had brought 39 enforcement actions against companies for alleged Safe Harbor violations, as well as an action against TRUSTe for allegedly misrepresenting the extent of its Safe Harbor assessments.

Finally, small and medium enterprises – which made up around 60 percent of Safe Harbor membership[15] –stand to lose the most from the *Schrems* decision. Like the biggest companies that are often discussed in public debates in Europe, these SMEs depend on the free flow of information to sell goods and services globally, build global workforces, and take advantage of low-cost cloud computing resources. Unlike the big companies, however, these SMEs do not have the time or resources to get BCRs approved or put model contractual clauses in place.

---

[14] *See* Dept. of Commerce, U.S.-EU Safe Harbor List, Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks, http://export.gov/safeharbor/ (last visited Dec. 9, 2015).

[15] *See* Dept. of Commerce – Int'l Trade Admin., Key Points Concerning the Benefits, Oversight, and Enforcement of Safe Harbor, *available at* https://build.export.gov/build/idcplg?IdcService=DOWNLOAD_PUBLIC_FILE&RevisionSelectionMethod=Latest&dDocName=eg_main_092414 (last visited Dec. 9, 2015).

These three losses, combined with the strong Constitutional, legislative, and administrative protections that the U.S. provides against government and private sector intrusions, provide a compelling case in support of reaching agreement on a new transatlantic framework soon.

In addition, looking further down the road, I see many privacy issues arising from the Internet of Things, big data analytics, and other developments. The FTC has begun to address them, but I think consumers and companies on both sides of the Atlantic will be better off if we have these conversations with our counterparts in Europe. Once we have a new transatlantic data transfer mechanism in place, we will all be in a much better position to do so.

While I wouldn't suggest that that's *all* you should want for Christmas, it wouldn't be a bad gift.

Thank you.