The Heritage Foundation

LEGAL MEMORANDUM

No. 194 | OCTOBER 27, 2016

The Federal Government's Appropriate Role in Internet Privacy Regulation

Alden F. Abbott

Abstract

The growth of the Internet economy has highlighted the costs associated with the unauthorized use of personal information transmitted online. The federal government's consumer protection agency, the Federal Trade Commission (FTC), has taken enforcement actions for online privacy violations based on its authority to proscribe "unfair or deceptive" practices affecting commerce. The FTC's economically influenced case-by-case approach to privacy violations focuses on practices that harm consumers. The Federal Communications Commission (FCC) has proposed a rule that would impose intrusive privacy regulation on broadband Internet service providers (but not other Internet companies), without regard to consumer harm. If implemented, the FCC's rule would impose major economic costs and would interfere with neutral implementation of the FTC's less intrusive approach, as well as the FTC's lead role in federal regulatory privacy coordination with foreign governments.

The Online Privacy Problem

While the Internet-based economy provides many benefits, it also raises new concerns for maintaining the privacy of information. "Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences."[1]

As the federal government's National Telecommunications and Information Administration (NTIA)[2] explains:

> Every day, billions of people around the world use the Internet to share ideas, conduct financial transactions, and keep in touch

This paper, in its entirety, can be found at **http://report.heritage.org/lm194**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Key Points

- The growth of the Internet economy has highlighted the costs associated with the unauthorized use of personal information transmitted online.
- The federal Government's consumer protection agency, the Federal Trade Commission (FTC), has taken enforcement actions for online privacy violations based on its authority to proscribe "unfair or deceptive" practices affecting commerce. The FTC's economically influenced case-by-case approach to privacy violations focuses on practices that harm consumers.
- The Federal Communications Commission (FCC) recently proposed a rule that would impose intrusive privacy regulation on broadband Internet service providers (but not other Internet companies), without regard to consumer harm.
- If implemented, the FCC's rule would impose major economic costs and would interfere with neutral implementation of the FTC's less intrusive approach, as well as the FTC's lead role in federal regulatory privacy coordination with foreign governments.

> with family, friends, and colleagues. Users send and store personal medical data, business communications, and even intimate conversations over this global network. But for the Internet to grow and thrive, users must continue to trust that their personal information will be secure and their privacy protected.

Internet privacy concerns are warranted. According to a July 2015 survey of Internet-using households,[3] 19 percent of such households (representing nearly 19 million households) reported that they had been affected by an online security breach, identity theft, or similar malicious activity during the 12 months prior to the survey. Security breaches appear to be more common among the most intensive Internet-using households—31 percent of those using at least five different types of online devices suffered such breaches. Security breach measures, of course, do not take into account consumer concerns about the unauthorized use of the personal data they supply to Internet service providers and to websites that they visit.

Furthermore, the total cost of data breaches is enormous.[4] A 2016 survey of corporate data breaches funded by IBM showed that the average annual per-company cost of data breaches rose from $3.8 million to $4.0 million between 2014 and 2015.[5] A 2014 study estimated that the aggregate annual data breach-specific cost to the U.S. economy was $140 billion (including direct costs to businesses, indirect costs to their customers, and indirect law enforcement-related costs), and that 500,000 jobs a year were lost due to such breaches.[6]

Online security failures often result in identity theft. The U.S. Federal Trade Commission (FTC) explains, "identity theft occurs when someone uses or attempts to use the sensitive personal information of another person to commit fraud. A wide range of sensitive personal information can be used to commit identity theft, including a person's name, address, date of birth, Social Security number (SSN), driver's license number, credit card and bank account numbers, phone numbers, and even biometric data like fingerprints and iris scans."[7] According to the U.S. Justice Department's Bureau of Justice Statistics, "an estimated 17.6 million Americans—about 7% of U.S. residents age 16 or older—were victims of identity theft in 2014."[8]

Some examples highlight the scale and the nature of the damage identity theft inflicts on consumers and businesses. For example, a 2013 hack of Target involved the theft of 40 million credit card records, leading to $443 million in losses for that company, a $1 billion fine, and substantial costs to customers whose credit card information was compromised.[9] In another case, AOL publicized the search history of 658,000 consumers from which those consumers could reportedly be identified.[10]

Information can be stolen if companies do not pay enough attention to the red flags of possible software problems. For example, Sony incorporated a copy-protection technology called XCP into the CDs it produced. As a side effect of this technology, it became possible to track consumer IP addresses, thereby undermining the security of these personal devices.[11] Depending upon the privacy settings and policies of social media and online dating sites, one's individual photos and name may be readily available through general online search engines for an indefinite period of time.[12] Several social media sites have also had scandals that involve the tracking of consumers. According to *The Wall Street Journal*, Foursquare, purveyor of a mobile app that allows one to learn about popular dining spots near one's current location, continues to track users' every movement—even after the app has been closed.[13]

Public attention has focused primarily on Internet data breaches by third party hackers and thieves, since the financial harm stemming from those harmful actions (and, in particular, identity theft), can be estimated. Nevertheless, government regulators are also concerned about other sorts of misuses of sensitive non-public consumer information that is obtained online—even when particularized financial losses cannot readily be measured. Perhaps the most severe such misuse involves the stalking of individuals by predators who obtain private information online (either directly from vulnerable individuals such as children and teenagers, or through data breaches).[14] Less obviously harmful are online companies' unauthorized uses of consumers' private data to make money through the sale of that information to advertisers and other commercial websites, or through the tracking of consumers' physical movements or web browsing patterns. Some consumers (although not all) may strongly resent and feel themselves harmed by such types of behavior, even if it does not result in direct out-of-pocket

losses. Such a concern is in harmony with the long-recognized legal American doctrine that individuals have a limited "privacy interest" in preventing certain personal information from being publicized.[15]

What is the correct overall approach government should take in dealing with Internet privacy problems? In addressing this question, it is important to focus substantial attention on the effects of such regulation on economic welfare. In particular, policies should address Internet privacy problems in a manner that does not unduly harm the private sector or deny opportunities to consumers. The U.S. Federal Trade Commission (FTC), the federal government's primary consumer protection agency, has been the principal federal regulator of online privacy practices. Very recently, however, the U.S. Federal Communications Commission (FCC) has asserted the authority to regulate the privacy practices of broadband Internet service providers, and is proposing an extremely burdensome approach to such regulation that would, if implemented, have harmful economic consequences. Congress may wish to take this into account in deciding whether to reallocate and constrain regulatory responsibilities in this area, which is so important to the 21st century innovation-driven economy.

The FTC and Privacy[16]

The FTC uses a variety of legal instruments in protecting consumers, and, in particular, individuals' privacy. As the FTC explains:

> The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. This broad authority allows the Commission to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models.
>
> The FTC uses a variety of tools to protect consumers' privacy and personal information. The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior. This includes, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust notice and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule. To date, the Commission has brought hundreds of privacy and data security cases protecting billions [sic] of consumers.[17]

More specifically, "[t]he FTC has brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware,[18] peer-to-peer file sharing, and mobile. These matters include over 130 spam and spyware cases and more than 50 general privacy lawsuits."[19] A very large portion of these matters involved online commercial activity.

As stated above, most of the FTC's privacy-related work is based on its core general authority to proscribe unfair or deceptive acts or practices under Section 5(a)(1) of the Federal Trade Commission Act (Section 5).[20] Although deception and unfairness are covered in the same statutory section, they represent different concepts.

The FTC defines "deception" as involving a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[21] Thus, deception occurs only when business conduct causes tangible harm to consumers who acted reasonably and were, nonetheless, misled. By comparison, conduct is "unfair" if it involves "an act or practice [that] causes or is likely to cause substantial injury to consumers which is not reasonably avoided by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[22] This necessarily calls for cost-benefit analysis, since it weighs potential efficiencies against consumer harm,

which makes it a more stringent test than deception.[23] Central to both the "deception" and "unfairness" cases is the concept of "materiality," which means that the behavior under scrutiny must actually affect consumer choices—if consumer choices are unaffected, consumers are not harmed, and thus the behavior does not violate Section 5. In a speech on Internet privacy protection, FTC Commissioner Maureen Ohlhausen summarized the interplay between Section 5 unfairness and deception:

> [U]nfairness establishes a baseline prohibition on practices that the overwhelming majority of consumers would never knowingly approve. Above that baseline, consumers remain free to find providers that match their preferences, and our deception authority governs those arrangements. . . . The FTC's case-by-case enforcement of our unfairness authority shapes our baseline privacy practices. Like the common law, this incremental approach has proven both relatively predictable and adaptable as new technologies and business models emerge.[24]

A brief review of representative Section 5 privacy cases provides a sense of how the FTC applies the unfairness and deception standards in that context. Applying these standards, the FTC has successfully resolved investigations (through settlements and final litigated decisions) in which it alleged that companies made deceptive claims about how they collect, use, and share consumer data; failed to provide reasonable security for consumer data; deceptively tracked consumers online; spammed and defrauded consumers; installed spyware or other malware on consumers' computers; shared highly sensitive, private consumer data with unauthorized third parties; and publicly posted such data online without consumers' knowledge or consent.[25] The many companies under FTC orders include Microsoft, Facebook, Google, Equifax, HTC, Twitter, Snapchat, and Wyndham Hotels.[26]

Although various specialized statutes (such as the Children's Online Privacy Protection Act) require special privacy frameworks for the conduct they cover, the general FTC Act does not legally obligate companies to produce an online privacy policy. Nevertheless, most foreign jurisdictions (including the European Union) and individual U.S. states (such as California) require that commercial website operators that collect personally identifiable data have such policies.[27] Thus, it makes sense for U.S. commercial providers to develop and post their policies regarding their data collection and dissemination practices.

For companies that adopt and post online privacy policies, a further issue is whether they decide to offer website users the choice of "opt in" or "opt out" information sharing frameworks. (Companies may choose to do neither and merely describe their privacy practices.) Under opt in, personal information obtained from website visitors cannot be shared with third parties (such as advertisers or marketers) unless and until the individual visiting a website grants permission for such use, typically by checking a box on a notice provided by the website. Under opt out, personal information can be shared unless the individual specifically requests that the website not do so. By its nature, opt in tends to restrict the dissemination of information, while opt out promotes more liberal information sharing. This difference is the result of the fact that many consumers may choose not to have their information shared if they have to make an initial election under opt in, while many consumers may not bother to act affirmatively to prevent information sharing under opt out.

Opt-in and opt-out policies also pose a welfare trade-off. The "up-front reminder" provided by opt in policies will be beneficial to consumers who highly value their privacy. But less privacy-sensitive consumers who value more highly the extra online services that are financed by websites' greater ability to monetize consumer information (by selling it to third parties) would benefit from opt out policies. In addition to these general considerations, the greater the sensitivity and potential consumer harm that may arise from a website's transfer of personal information, the more likely opt in policies will prove beneficial for the bulk of that website's customers. In reviewing complaints in this area (for example, the claim that a company has sold the private information of consumers who opted against information sharing), the FTC applies its general Section 5 deception and unfairness principles on a case-by-case basis.[28]

The FCC Steps In

Until very recently, the FTC was the only federal agency scrutinizing online privacy practices. On

April 1, 2016, however, the FCC, which is the federal communications regulatory agency,[29] published a Notice of Proposed Rulemaking (NPRM) entitled "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services."[30] This "Privacy NPRM" sets forth detailed rules that, if adopted, would impose onerous privacy obligations on "Broadband Internet Access Service" (BIAS) Providers, the firms that provide the cables, wires, and telecommunications equipment through which Internet traffic flows—primarily cable (Comcast, for example) and telephone (Verizon, for example) companies.[31] The Privacy NPRM reclassifies BIAS provision as a "common carrier" service, thereby totally precluding the FTC from regulating BIAS Providers' privacy practices (since the FTC is barred by law from regulating common carriers).[32] Put simply, the NPRM required BIAS Providers "to obtain express consent in advance of practically every use of a customer['s] data,"[33] without regard to the effects of such a requirement on economic welfare. All other purveyors of Internet services, however—in particular, the large numbers of "edge providers" that generate Internet content and services (Google, Amazon, and Facebook, for example) —are exempt from the new FCC regulatory requirements.

In short, the Privacy NPRM establishes a two-tier privacy regulatory system, with BIAS Providers subject to tight FCC privacy rules, while all other Internet service firms are subject to more nuanced, case-by-case, effects-based evaluation of their privacy practices by the FTC. This disparate regulatory approach is peculiar (if not wholly illogical), since edge providers in general have greater access than BIAS Providers to consumers' non-public information, and thus may appear to pose a greater threat to consumers' interest in privacy.[34]

The FCC's proposal to regulate BIAS Providers' privacy practices represents bad law and bad economic policy, in several respects.

First, the Privacy NPRM undermines the rule of law by extending the FCC's authority beyond its congressional mandate. The FCC justifies its privacy rules by invoking Section 222 of the Telecommunications Act of 1996,[35] which empowers the FCC to regulate information Customer Proprietary Network Information (CPNI) over *voice telephony*. CPNI only covers a narrow category of information—telecommunications providers' collection and use of individualized subscriber information regarding the time and length of calls, phone numbers called, and consumer voice billing when such information "is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[36] By contrast, the Privacy NPRM proposes to regulate the far broader category of "personally identifiable information," or PII, defined as information that "can be used on its own, in context, or in combination to identify an individual or to logically associate with other information about a specific individual."[37]

In short, under the NPRM, the FCC cites its authority over a very limited category of "telephone bill" information unrelated to Internet communications to justify regulating vast amounts of private information transmitted over the Internet. This is "a gross overextension of the authority conferred by Congress under Section 222. It is legally improper for the Commission to reinterpret its circumscribed privacy mandate regarding telephone services and overextend that authority to the competitive broadband services."[38] Moreover, this expansive approach is at odds with the overall guidance Congress provided the FCC in enacting the 1996 Telecommunications Act, which emphasizes reliance on competitive forces, rather than FCC regulation,[39] and provides for FCC forbearance from regulating telecommunications services to the greatest extent possible,[40] including when regulation "is not necessary for the protection of consumers."[41]

Second, the Privacy NPRM imposes a set of sweeping opt-in consent requirements on BIAS Providers, without regard to private sector burdens or actual consumer welfare.[42] In the name of protecting online privacy, the NPRM requires that BIAS Providers seek affirmative opt-in consent from each customer for virtually all uses of any consumer data.[43] A BIAS Provider would have to inform customers of its intended use of their data and then obtain their consent—even if the Provider had no plans to disclose the data and even if the data already was being used by other Internet businesses for advertising and marketing purposes. In contrast, the FTC has reserved its imposition of opt-in requirements to very limited situations, involving "specific uses like making retroactive changes to privacy representations, or collecting sensitive information, such as information about children, financial and health information, Social Security numbers, and precise geolocation data."[44] The FTC's limited use of opt-in requirements reflects the fact that "opt in mandates

unavoidably reduce consumer choice" by setting a privacy baseline that is too high and by preventing unanticipated beneficial uses of consumer data.[45] In a similar vein, former FTC Commissioner Joshua Wright wrote that the Privacy NPRM imposes "a rigid, one-size-fits-all regulatory approach, forgoing the individualized analyses that leave space for innovative, welfare-enhancing uses of customer information."[46] In particular, Wright aptly summarized the nature of the costs the FCC's approach would impose on consumers and the economy as a whole:

> [The Privacy NPRM] presumes that consumers with strong privacy preferences somehow cannot effectively protect these interests by opting-out when doing so would make them better off, and, instead, imposes the burdens to act upon those consumers with weak preferences. Far from benefiting consumers, this regime eliminates the ability of firms to compete and experiment with business models to maximize consumer value and would impose significant costs upon many firms in the online ecosystem—costs that consumers would ultimately bear. These costs would far outweigh the very limited and speculative benefits the NPRM proffers.[47]

Third, the Privacy NPRM, if implemented, will reduce BIAS Provider revenues and thereby dampen investment that is vital to the continued growth of and innovation in Internet-related industries. Opt-in restrictions will sharply limit the ability of BIAS Providers to monetize consumer information by selling it to advertisers and marketers, thereby reducing funds available to finance new Internet services and improving existing services. Furthermore, the financial health of BIAS Providers would be undermined. As the U.S. Chamber of Commerce explained, in its comment on the Privacy NPRM:

> The NPRM threatens the long-term economic health of broadband and other telecommunications providers. According to Moody's Investors Services, the FCC's proposed privacy rules pose "a long-term risk to the current TV advertising business model, as well as all broadband providers whom also have ad sales exposure." Given the regulatory imbalance created by the proposed rule, the credit agency also predicts that NPRM will be "credit-negative" for Internet service providers.[48]

Fourth, and relatedly, Edge providers (Google, for example), which are not covered by the NPRM (and whose ability to monetize consumer information is subject only to "lighter touch" FTC oversight), will feel less competitive pressure from BIAS Provider offerings, and have a weaker incentive to innovate and compete in Internet service provision.[49]

Fifth, the Privacy NPRM, if implemented, will harm consumer welfare and, in particular, raise consumer prices for Internet services and deny discount programs desired by consumers. NPRM-related limitations on the ability of BIAS Providers to monetize consumer data will, by reducing advertising revenue used to help defray broadband service costs, incentivize the Providers to raise consumer broadband service prices.[50] In addition, by barring BIAS Providers from offering discounted Internet broadband services in exchange for greater access to consumer data, the NPRM will deny a valuable option to consumers who value service discounts more than additional data privacy.[51]

In sum, the Privacy NPRM would, if implemented, undermine the economic welfare of both businesses and consumers in a manner that ignores clear limitations on the FCC's statutory authority. As a matter of sound economics and law, the FCC should abandon this disastrous proposal and leave the federal oversight of online Internet privacy where it now resides—with the FTC.

International Considerations

While the previous discussion has centered on the federal government's approach to Internet privacy, foreign governments increasingly have sought to regulate privacy (and, in particular, data protection) practices,[52] generally in a far more intrusive manner than that employed by the FTC. Because the Internet is global in scope, American businesses (particularly those with a significant international reach) need to take into account foreign privacy regulations in planning their operations.

The U.S. government has negotiated with the European Union (EU),[53] the multi-jurisdictional entity with the most comprehensive privacy policy, in seeking to avoid excess burdens on private entities. On February 2, 2016, the EC (the European Union's administrative and regulatory body)[54] and the U.S. government agreed on a new regulatory framework covering transatlantic exchanges of personal data for commercial purposes (for example, bank or corporate transmissions of such

data)—the EU-U.S. Privacy Shield.[55] The Privacy Shield responded to a 2015 European Court of Justice ruling invalidating a prior EU-U.S. "Safe Harbor" Agreement for dealing with data exchange.[56] The Shield allows companies to subject themselves to specified principles governing their U.S.-EU and EU-U.S. data transfer. (Notably, the FTC, *not* the FCC, played a key role in Privacy Shield negotiations and is endowed with significant Shield-related enforcement responsibilities.) Key elements of the agreement include:

1. **Commitments by Companies to Robust Data Protection**. U.S. companies participating in the new framework will be required to commit to robust obligations regarding the processing of personal data from Europe. Companies handling human resources data from Europe will be further required to agree to comply with the decisions of the Data Protection Authorities ("DPAs") of the various EU member states.

2. **FTC Enforcement**. The [FTC]...will have enforcement authority regarding U.S. companies' compliance with the new framework, just as it did with the old Safe Harbor agreement. The U.S. Department of Commerce will have overall responsibility for monitoring companies' compliance with the Privacy Shield framework.

3. **Redress for EU Citizens**. EU citizens who believe that their data has been misused by a U.S. company will have several avenues of redress. For example, DPAs may refer EU citizen complaints to the Department of Commerce and the FTC. In addition, a new Ombudsperson will be established to handle complaints of access to personal data by national intelligence authorities.

4. **Restrictions on U.S. Government Surveillance**. Access to EU personal data by U.S. law enforcement and national security authorities will be subject to clear limitations and oversight, and the U.S. has provided the EU with written assurances to this effect. The absence of such protections was a key factor in the...[European Court of Justice's 2015] decision that invalidated the Safe Harbor agreement. The European Commission and the U.S. Department of Commerce will conduct annual joint reviews regarding the issue of national security access.[57]

Membership in the Privacy Shield is entirely voluntary. In deciding whether to bring themselves under the Shield, which imposes significant and costly regulatory obligations and severe sanctions for violations of Shield commitments, American businesses may wish to consider instead using standardized contractual terms to govern their U.S.-EU data transfers.[58] Whether or not they "opt in" to Shield commitments, however, American firms doing business in the EU will be subject to potentially large and uncertain liability and European regulatory oversight.

Furthermore, given the very significant influence of European data protection and privacy norms on international thinking,[59] the implementation and evolution of Shield and European DPA policies will be a major ongoing concern for American companies, wherever they do business. The Privacy NPRM (if implemented) heightens that concern for BIAS Providers, since they will have to evaluate the implications of new FCC regulation (rather than simply rely on FTC oversight) in deciding whether to opt in to the Shield's standards and obligations.

Recommendations

The FCC's Privacy NPRM is at odds with the procompetitive, economic welfare enhancing goals of the 1996 Telecommunications Act. It ignores the limitations imposed by that act and, if implemented, would harm consumers and producers and slow innovation. This prompts four recommendations.

- The FCC should withdraw the NPRM and leave it to the FTC to oversee all online privacy practices under its Section 5 unfairness and deception authority. The adoption of the Privacy Shield, which designates the FTC as the responsible American privacy oversight agency, further strengthens the case against FCC regulation in this area.

- In overseeing online privacy practices, the FTC should employ a very light touch that stresses economic analysis and cost-benefit considerations. Moreover, it should avoid requiring that rigid privacy policy conditions be kept in place for long periods of time through consent decree conditions, in order to allow changing market conditions to shape and improve business privacy policies.

- Moreover, the FTC should borrow a page from former FTC Commissioner Joshua Wright by

implementing an "economic approach" to privacy.[60] Under such an approach:

- FTC economists would help make the commission a privacy "thought leader" by developing a rigorous academic research agenda on the economics of privacy, featuring the economic evaluation of industry sectors and practices;
- The FTC would bear the burden of proof in showing that violations of a company's privacy policy are material to consumer decision-making;
- FTC economists would report independently to the FTC about proposed privacy-related enforcement initiatives; and
- The FTC would publish the views of its Bureau of Economics in all privacy-related consent decrees that are placed on the public record.

- The FTC should encourage the European Commission and other foreign regulators to take into account the economics of privacy in developing their privacy regulatory policies. In so doing, it should emphasize that innovation is harmed, the beneficial development of the Internet is slowed, and consumer welfare and rights are undermined through highly prescriptive regulation in this area (well-intentioned though it may be). Relatedly, the FTC and other U.S. government negotiators should argue against adoption of a "one-size-fits-all" global privacy regulation framework.[61] Such a global framework could harmfully freeze into place over-regulatory policies and preclude beneficial experimentation in alternative forms of "lighter-touch" regulation and enforcement.

Although not a panacea, these recommendations would help deter (or, at least, constrain) the economically harmful government micromanagement of businesses' privacy practices in the United States and abroad. The Internet economy would in turn benefit from such a restraint on the grasping hand of big government.

*—**Alden F. Abbott** is Deputy Director of and John, Barbara, and Victoria Rumpel Senior Legal Fellow in the Edwin Meese III Center for Legal and Judicial Studies at The Heritage Foundation. He gratefully acknowledges the research assistance of Heritage Foundation Intern Jessica Higa, who participated in the Young Leaders Program.*

Endnotes

1. *Internet Privacy*, TECHOPEDIA.COM, https://www.techopedia.com/definition/24954/internet-privacy (last visited Aug. 18, 2016).
2. NTIA is the Executive Branch agency that is principally responsible by law for advising the President on telecommunications and information policy issues. *About NTIA*, NTIA.GOV, https://www.ntia.doc.gov/about (last visited Aug. 18, 2016).
3. *See* Rafi Goldberg, *NTIA, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA BLOG (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.
4. For a comprehensive chronological summary of data breaches suffered by businesses, *see eg.*, *Chronology of Data Breaches/Security Breaches 2005 – Present* (2016), PRIVACY RIGHTS, http://www.privacyrights.org/data-breach (last visited Aug. 19, 2016).
5. *See* Ponemon Institute, *2016 Cost of Data Breach Study: Global Analysis*, IBM (June 2016), http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN.
6. Matthew Zajechowski, *How Consumers Foot the Bill for Data Breaches*, SMART DATA COLLECTIVE, http://www.smartdatacollective.com/matthew-zajechowski/223676/how-consumers-foot-bill-data-breaches.
7. *Guide for Assisting Identity Theft Victims*, FTC (Sept. 2013), https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.
8. *Victims of Identity Theft*, BUREAU OF JUSTICE STATISTICS (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14_sum.pdf.
9. *See id*.
10. Michelle Kessler & Kevin Maney, *AOL's Tech Chief Quits After Breach of Privacy,* USA TODAY (Aug. 21, 2006), http://usatoday30.usatoday.com/tech/news/Internetprivacy/2006-08-21-aol-privacy-departures_x.htm.
11. *See* Fred Von Lohmann, *Are You Infected by Sony-BMG's Rootkit?*, ELECTRONIC FRONTIER FOUNDATION (Nov. 8, 2005), https://www.eff.org/deeplinks/2005/11/are-you-infected-sony-bmgs-rootkit.
12. *See* Rainey Reitman, *Six Heartbreaking Truths about Online Dating Privacy*, ELECTRONIC FRONTIER FOUNDATION (Feb. 10, 2012), https://www.eff.org/deeplinks/2012/02/six-heartbreaking-truths-about-online-dating-privacy.
13. Douglas MacMillan, *Foursquare Now Tracks Users Even When the App is Closed*, WALL ST J. (Aug. 6, 2014), http://blogs.wsj.com/digits/2014/08/06/foursquare-now-tracks-users-even-when-the-app-is-closed/.
14. *See*, *e.g.*, *Children & Teen Statistics*, ONLINESENTRY, http://www.sentrypc.com/home/statistics.htm (last visited Aug. 18, 2016); *Sexual Exploitation & Abuse/Child Porn*, ENOUGH IS ENOUGH, http://enough.org/stats_exploitation (last visited July 12, 2016); *Online Predator Statistics and Facts*, KEYLOGGER REVIEW (May 21, 2016), http://keyloggers.mobi/online-predator-statistics/ (citing statistics regarding exposure by teens and children to online pornography and online sexual solicitations, and related online stalking problems).
15. The first noteworthy scholarly discussion of an individual "right to privacy" under Anglo-American law is Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193 (1890), http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.
16. For a detailed discussion of the appropriate FTC's role in regulating online data security, an important aspect of privacy, *see* Alden Abbott, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?*, HERITAGE FOUNDATION LEGAL MEMORANDUM No. 137 (Sept. 10, 2014), http://www.heritage.org/research/reports/2014/09/the-federal-trade-commissions-role-in-online-security-data-protector-or-dictator#_ftn1. This memorandum deals more generally with online privacy.
17. FTC, PRIVACY & DATA SECURITY UPDATE (Jan. 2016), https://www.ftc.gov/reports/privacy-data-security-update-2015#privacy. *See also id*. for more detail on the Fair Credit Reporting Act, the Children's Online Privacy Protection Act, and the Telemarketing Sales Rule.
18. Spyware involves the insertion of a software "virus" that can monitor or control your computer use. It may be used to send consumers pop-up ads, redirect their computers to unwanted websites, monitor their Internet surfing, or record their keystrokes, which, in turn, could lead to identity theft. *Combating Spyware and Malware*, FTC, https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware (last visited Aug. 19, 2016).
19. FTC, PRIVACY & DATA SECURITY, *supra* note 17.
20. 15 U.S.C. § 45(a)(1).
21. James C. Miller III, Chairman, FTC, Policy Statement on Deception to The Honorable John D. Dingell, Chairman, Energy and Commerce, U.S. House of Representatives (Oct. 14, 1983), appended to Clifford Associates, Inc., 103 F.T.C. 110, 174 (1984), http://www.ftc.gov/ftc-policy-statement-on-deception.
22. 15 U.S.C. § 45n.
23. *See*, *e.g.*, J. Howard Beales III, Director, Bureau of Consumer Protection, FTC, Address at the Marketing and Public Policy Conference: The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003), http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection. Current FTC Commissioner Josh Wright also has stressed the importance of cost-benefit analysis. *See, e.g.,* Joshua D. Wright, Commissioner, FTC, Remarks to the George Mason University Law & Economics Center and Alliance of California Judges: The Economics of Access to Civil Justice: Consumer Law, Mass Torts, and Class Actions (Mar. 16, 2014), http://www.ftc.gov/system/files/documents/public_statements/293621/140316civiljustice-wright.pdf.

24. Maureen K. Ohlhausen, Commissioner, FTC, Remarks at the Free State Foundation Eighth Annual Telecom Policy Conference: Privacy Regulation in the Internet Ecosystem 4–5 (Mar. 23, 2016), https://www.ftc.gov/system/files/documents/public_statements/941643/160323fsf1.pdf. Former FTC Commissioner Joshua Wright has expressed some skepticism about the FTC.
25. *See Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission to the Federal Communications Commission*, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, FCC 16-39, at 4-5 (May 27, 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.
26. *Id*. at 5.
27. *See Privacy Policies Are Required Everywhere*, Iubenda, http://www.iubenda.com/en/privacy-legal-requirements (accessed Aug. 19, 2016).
28. Former FTC Commissioner Joshua Wright has expressed concern that FTC consumer protection analysis in general, and privacy analysis in particular, are insufficiently attuned to economic considerations, in particular, the "tradeoffs between the value to consumers and society of the free flow and exchange of data and the creation of new products and services on the one hand, against the value lost by consumers from any associated reduction in privacy." Joshua D. Wright, *The FTC and Privacy Regulation: The Missing Role of Economics*, George Mason University Law & Economics Ctr 7 (Nov. 12, 2015), http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.
29. The FCC is an independent federal government agency charged by Congress with "regulating] interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories." *The FCC's Mission*, FCC, https://www.fcc.gov/about/overview (last visited Aug. 19, 2016).
30. FCC, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106 (released Apr. 1, 2016), WC Docket No. 16-106, https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf. Consistent with the Administrative Procedure Act, an NPRM soliciting public comments on a proposed rule may be followed by the FCC's issuance of a final binding rule. See *Rulemaking*, FCC, https://www.fcc.gov/general/rulemaking (last visited Aug. 19, 2016).
31. The Privacy NPRM defines BIAS as a "mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service." Privacy NPRM, *id.*, at ¶ 29.
32. *See* 15 U.S. Code § 45(a)(2) (the FTC's authority to prevent firms from using "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce" does not extend to "common carriers subject to the Acts to regulate commerce".
33. Harold Furchtgott-Roth & Arielle Roth, *The FCC Wants To Regulate Your Internet Privacy Now, Too*, Forbes (Mar. 14, 2016), http://www.forbes.com/sites/haroldfurchtgottroth/2016/03/14/why-the-fccs-proposed-privacy-rules-would-hurt-consumers/#32dca1ac4c49.
34. Edge provider websites such as Google and Amazon, unlike BIAS Providers, routinely request large amounts of consumer information. Moreover, a large proportion of the information transmitted through BIAS Provider networks (70 percent or higher by latest count) is encrypted, sharply limiting the ability of those Providers to misuse non-public consumer data. *See* Thomas Lenard & Scott Wallsten, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking*, Technology Policy Inst. (May 2016), https://techpolicyinstitute.org/wp-content/uploads/2016/05/Lenard_Wallsten_FCCprivacycomments.pdf.
35. 47 U.S.C. § 222.
36. 47 U.S.C. § 222(h)(1)(A).
37. Privacy NPRM, at ¶¶ 60, 61.
38. In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (released Apr. 1, 2016), Comments of the Free State Foundation, at 5 (May 27, 2016), http://www.freestatefoundation.org/images/FCC_Privacy_Comments_-_Final_052716.pdf.
39. *See*, *e.g.*, 47 U.S.C. preamble (the Act's single goals is "[t]o promote competition and reduce regulation"); 47 U.S.C. § 706(c) (the "Internet and other interactive computer services have flourished . . . with a minimum of government regulation"); and 47 U.S.C. § 257(b) (the FCC's mandate is to promote policies favoring "vigorous economic competition").
40. *See* 47 U.S.C. § 160 ("Competition in telecommunications service").
41. 47 U.S.C. § 160(a)(2).
42. This discussion draws heavily upon Gerald R. Faulhaber & Hal J. Singer, The Curious Absence of Economic Analysis at the Federal Communications Commission: An Agency in Search of a Mission 52–53 (July 2016 draft), http://www.calinnovates.org/curious-absence-economic-analysis-federal-communications-commission-agency-search-mission/ (accessed Aug. 19, 2016).
43. *See* Privacy NPRM ¶¶ 62, 127–133.
44. FCC NPRM, Dissenting Statement of FCC Commissioner Michael O'Rielly, at 3 (Apr. 1, 2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A6.pdf.
45. *See* Ohlhausen, *supra* note 24.
46. Joshua D. Wright, An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy 6 (May 27, 2016) (footnote reference deleted), https://www.ustelecom.org/sites/default/files/documents/ExParte_re_Wright_Privacy_FINAL.pdf.

47. *Id*. at 11 (footnote reference deleted).
48. Letter from the U.S. Chamber of Commerce to Marlene Dortch, Secretary, FCC, Commenting on the Privacy NPRM, at 6–7 (footnote references omitted), https://www.uschamber.com/sites/default/files/documents/files/5.26.16-_comments_to_fcc_on_proposed_broadband_privacy_rules.pdf.
49. *See* Faulhaber & Singer, *supra* note 42, at 53.
50. *See* Wright, *supra* note 46, at 6.
51. *See FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the Subcomm. on Communications and Technology of the H. Comm. on Energy & Commerce* 114th Cong., 2nd Sess. (2016) (Statement of Jon Leibowitz, Co-Chairman, 21st Century Privacy Coalition), http://docs.house.gov/meetings/IF/IF16/20160614/105057/HHRG-114-IF16-Wstate-LeibowitzJ-20160614.pdf (last visited Aug. 19, 2016).
52. *See, e.g.*, *What is Data Protection?* Privacy International, https://www.privacyinternational.org/node/44 (last visited Aug. 19, 2016); David Banisar, *National Comprehensive Data Protection/Privacy Laws and Bills 2016 Map* (Apr. 30, 2016) (compilation of over 100 jurisdictions with privacy/data protections laws), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 (last visited Aug. 19, 2016); *Data Protection Laws of the World*, DLA Piper (2016) (providing short summaries of different jurisdictions' laws), https://www.dlapiperdataprotection.com/#handbook/world-map-section (last visited Aug. 19, 2016).
53. *The EU in Brief*, European Union (May 13, 2016), http://europa.eu/about-eu/basic-information/about/index_en.htm. As of today, the EU comprises 28 European nations.
54. *See About the European Commission*, European Union (July 7, 2016), http://ec.europa.eu/about/index_en.htm.
55. *See* Press Release, European Commission, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016), http://europa.eu/rapid/press-release_IP-16-2461_en.htm. The EC formally adopted the Shield on July 12, 2016, making it immediately applicable within EU Member States.
56. *See id*.
57. *U.S. and EU Agree to New "Privacy Shield" Framework to Replace Safe Harbor*, Ice Miller LLP (Feb. 3, 2016), http://www.icemiller.com/ice-on-fire-insights/publications/u-s-and-eu-agree-to-new-privacy-shield-framework-t/.
58. *See* Aaron Tantleff, *To Join or Not to Join: Is the EU-U.S. Privacy Shield Right for You?* Foley & Lardner LLP (Apr. 11, 2016), https://www.foley.com/to-join-or-not-to-join-is-the-eu-us-privacy-shield-right-for-you/.
59. *See, e.g.*, Christopher Kuner, *The European Union and the Search for an International Data Protection Framework*, 2 Groningen J. Int'l L 55 (2014), https://groningenjil.files.wordpress.com/2015/04/grojil_vol2-issue2_kuner.pdf.
60. *See* Wright, *supra* note 28, for a discussion of such an approach.
61. Notably, the EU and other nations have called for a global data protection framework. *See* Kuner, *supra* note 59, at 56–61.