

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Protecting the Privacy of Customers of) WC Docket No. 16-106
Broadband and Other Telecommunications)
Services)

**COMMENTS
OF
THE AMERICAN CIVIL LIBERTIES UNION (“ACLU”)**

Submitted: May 27, 2016

Comments of the ACLU

The ACLU supports the proposal of the Federal Communications Commission (Commission) to apply the traditional privacy protections of the Communications Act to broadband Internet access service. Americans have the right to a telecommunications infrastructure where their privacy is protected. Application of longstanding privacy rules is necessary to allow the Commission to carry out its vital role in providing robust privacy protections for Internet connectivity.

For nearly 100 years, the ACLU has been our nation’s guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual’s rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

The ACLU’s views are well represented in the comments of the Consumer Federation of American and 17 other organizations and we agree with most of the specific elements set forth in that document.¹ However, in these separate comments we would like to additionally emphasize several issues that are of particular interest and concern to our organization and its members.

¹ Consumer Federation of America et al., Comment Letter on Proposed Rule on Protecting the Privacy of Customers of Broadband and other Telecommunications Services (May 27, 2015), <http://consumerfed.org/testimonial/cfa-urges-fcc-move-forward-rulemaking-process-protecting-broadband-consumers-privacy/>.

The right to privacy in communications

Americans expect and deserve to have access to a communications infrastructure where privacy is protected. The nation's mail, telephone, and telegraph infrastructures have long been subject to rules protecting that privacy. When an American picks up the phone to call a suicide hotline, an outreach service for gay teens, or a cancer doctor, he or she doesn't have to worry that the phone company will sell that information to others, thanks to section 222 of the Communications Act² which prohibits such privacy invasions. There is no reason why that same privacy protection should not apply to the internet, which has superseded the telephone system as the most important communications network in Americans' lives. Indeed, when Congress enacted § 222, it abandoned proposed language confining its application to telephone service, specifically expanding its scope to cover all telecommunications services.³ In so doing, Congress recognized that privacy protections should not hinge upon the specific technology people use to communicate. Why should Americans enjoy strong privacy protection when they communicate using analog fluctuations in electrical signals over copper wires, a 19th century technology, but not when they communicate using digital bits over the internet? The plain language of § 222 not only gives the FCC the authority to expand privacy protections to broadband internet access service (BIAS) providers, it requires it.

Confidentiality and control over the information about oneself that one allows to disseminate are an inherent part of human life, and privacy is a core human need. When communications media are not regarded as trustworthy and private, people seek out other means of communicating. If we as a society create a telecommunications infrastructure where privacy is not protected, then many people and businesses will seek out alternative, less efficient means of communicating, rendering that infrastructure *less valuable* to them and to society.

A telecommunications infrastructure that is not regarded as solidly trustworthy and private will also create significant chilling effects on self-expression. The internet has become the primary communications medium of our age, and no one can fully experience modern life and participate in democratic self-governance without being free to not only publish and broadcast online, but also to engage in confidential communications and organizing efforts. Those who cannot do these things are lacking a key freedom that all Americans should enjoy — a freedom that has played a crucial role in supporting the artistic, intellectual, and social vitality of our nation, and therefore its economic vitality as well.

Several studies carried out in the wake of the Snowden revelations about NSA spying have documented the chilling effects that surveillance can have on freedom of expression. A 2016 study published in the peer-reviewed journal *Journalism and Mass Communication Quarterly* found a significant suppression in subjects' willingness to express nonconformist views when given cues priming them to believe they were under surveillance by the government.⁴ A 2013

² 47 U.S.C §222.

³ HAROLD FELD ET. AL., PROTECTING PRIVACY, PROMOTING COMPETITION: A FRAMEWORK FOR UPDATING THE FEDERAL COMMUNICATIONS COMMISSION PRIVACY RULES FOR THE DIGITAL WORLD 15 (2016).

⁴ Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence in the Wake of NSA Internet Monitoring*, JOURNALISM & COMMUNICATION QUARTERLY, 1 (2016), <http://m.jmq.sagepub.com/content/early/2016/02/25/1077699016630255.full.pdf?ijkey=1jxrYu4cQPtA6&keytype=ref&siteid=spjmq>.

study published by the PEN American Center found self-censorship widespread among writers as a result of heightened awareness of online monitoring,⁵ and a 2014 Pew survey of 1,801 American adults found an increased hesitancy to discuss the NSA online.⁶ A 2016 study published in the *Berkeley Law Journal* found chilling effects among Wikipedia users after the Snowden revelations,⁷ and a 2015 study found changes in Google users' search behavior.⁸ A variety of political groups and activists have also testified in legal proceedings that they have felt chilling effects from such surveillance.⁹

Although many of these studies were conducted in the context of NSA surveillance, which is an entirely separate issue from that of monitoring by BIAS providers, there is every reason to believe that the same psychological dynamics of surveillance will come into play if internet users come to believe that their online traffic is susceptible to routine monitoring by their carriers.

BIAS providers ask that the FCC not enforce the law because they wish to grab short-term profits by eavesdropping on communications, as they look jealously at booming online companies such as Google and Facebook, as well as an entire ecology of online advertising companies, which are enjoying a boom at the moment. But the broadband providers are clearly covered by the protections for those communicating over common carriers that is afforded by § 222, and the edge providers are not. And there is a fundamental difference between the edge destinations that people choose to use online, and can abandon for a competitor virtually at the click of a mouse, and the internet infrastructure itself. BIAS providers have the potential to monitor not just one area of a customer's internet use, but all of them. In addition, the state of competition among BIAS providers (oligopolistic at best) is such that the providers have significant market power, and even where equivalent competitive options are available, the switching costs can be considerable.

Furthermore, the online ecosystem is a fluid, rapidly changing environment, where consumers can stampede from one web service to another at a whim, where empires rise and fall seemingly overnight (for example Myspace, Friendster, Netscape, RealNetworks, Orkut, and Digg), or across a decade (for example AOL or Yahoo). While some communications infrastructures have been regularly spied upon from time to time throughout history, in the end people need, and always demand, privacy. As historian David Kahn put it, invasions of privacy contradict "a long evolution toward the secrecy of communications. Centuries ago, people in England, France and the German states fought for the right to send letters without their being opened by the 'black chambers' of absolutist monarchs." Across Europe, Kahn writes,

⁵ PEN AMERICA, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR (2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

⁶ Elizabeth Dwoskin, *Survey: People Don't Want to Talk Online About the NSA*, W.S.J., Aug. 26, 2014, <http://blogs.wsj.com/digits/2014/08/26/survey-people-dont-want-to-talk-online-about-the-nsa/>.

⁷ Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKLEY TECH. L. J. (forthcoming 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.

⁸ Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564.

⁹ *First Unitarian Church of Los Angeles v. National Security Agency*, 2014 WL 4693046 (N.D.Cal.) (Trial Pleading) (Declarations of Plaintiffs), <https://www.eff.org/files/2013/11/06/allplaintiffsdeclarations.pdf>.

the public knew about the letter-opening and hated it. The pre-revolutionary French assembly, the Estates-General, received complaints from all regions of France and from all classes of society about this invasion of their thoughts. A month after the fall of the Bastille, Article 11 of the Declaration of the Rights of Man held that citizens may write with freedom — in effect nullifying the right of the government to read letters. In the United States, the 1792 law establishing the Post Office forbade its agents from illegally opening the mail entrusted to it.¹⁰

In 1794 Prussia enacted a law punishing letter-opening, Kahn writes, and “other states of Germany and elsewhere in Europe followed.” In 1844 the British Parliament “exploded” when an Italian visitor learned his letters had been opened, and the resulting “uproar” ended the practice.

More recently, revelations about wholesale spying by the NSA have created a new firestorm of controversy—and a worldwide movement toward increasing the protection of privacy through both political and technological means.

In the end, people need and will demand privacy.

Often there is a lag, sometimes substantial, between when people first lose their privacy and when they begin to understand and resent that loss, and demand its correction. It is just this lag that the advertising industry is currently depending upon in today’s online edge-provider ecosystem. But this ecosystem, in which millions of people appear to have traded their privacy for free online services, evokes profound discomfort in many people, according to numerous polls.¹¹

In short, while many industry players would like to proclaim the advent of a “new era” in which privacy matters less, nothing could be further from the truth. The FCC must not let the essentially corrupt practices that dominate our online ecosystem at the current moment in time be imported into the essential communications infrastructure in which that ecosystem lives. If edge providers are software, the broadband providers are the hardware on which that software runs—and corruption of privacy in the hardware will prove much harder to correct.

The Commission asks many questions in its NPRM, and we regret that we do not have the capacity to weigh in on all of them. We do believe that overall, privacy should be protected to the strongest possible extent. Below we offer comments on selected questions for which the Commission has solicited public feedback.

¹⁰ David Kahn, *Back When Spies Played by the Rules*, N.Y. TIMES, Jan. 13, 2006, <http://www.nytimes.com/2006/01/13/opinion/13kahn.html>.

¹¹ See, e.g. Marc Fisher & Craig Timberg, *American Uneasy About Surveillance but Often Use Snooping Tools, Post Poll Finds*, WASH. POST, Dec. 21, 2013, https://www.washingtonpost.com/world/national-security/americans-uneasy-about-surveillance-but-often-use-snooping-tools-post-poll-finds/2013/12/21/ca15e990-67f9-11e3-ae56-22de072140a2_story.html; Edward Baig, *Internet Users Say, Don’t Track Me*, U.S.A. TODAY, Dec. 14, 2010, http://usatoday30.usatoday.com/money/advertising/2010-12-14-donottrackpoll14_ST_N.htm; JOSEPH TUROW ET. AL., *CONTRARY TO WHAT MARKETERS SAY, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT* (2009), https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

Limiting collection, retention, and disposal of data

The Commission asks whether it should impose reasonable limits not only on the use of customer information by carriers, but also on the collection and retention of such data. In our view, the answer is yes. There are several reasons for this.

First, data security. As the renowned cryptographer and security expert Bruce Schneier has put it, “For a lot of reasons, computer and network security is very difficult. Attackers have an inherent advantage over defenders, and a sufficiently skilled, funded and motivated attacker will always get in.”¹² Given this reality of the computer age, there is ample justification for forbidding the telecom carriers from not only *using* customer information for purposes unrelated to the provision of service, but also from *storing* such information for purposes unrelated to the provision of any service that customers have meaningfully opted in to. As Schneier put it, “data is a toxic asset and saving it is dangerous.”¹³ A potential data breach would not only have grave consequences for consumer privacy, it could also pose a threat to our national security by exposing sensitive information about millions of Americans, including federal employees or government contractors, to malicious actors. Thus, limits on data retention are necessary to give substance to the statutory requirement that telecommunications carriers “protect the confidentiality of proprietary information of, and relating to... customers.”¹⁴

Second, and relatedly, the kind of massive and intrusive data collection practices that would be entirely permissible in the absence of a rule to the contrary would violate consumers’ expectations. Consumers who are paying for internet service do not expect their carriers to be compiling information about their medical conditions, their online reading habits, their financial interests, or their taste in pornography. As the Commission notes, limiting data retention is one of the Fair Information Practice Principles recognized around the world as a core element of a fair approach to handling information, and the carriers have no business recording their customers’ tastes, interests, associations, and activities. To allow them to do so would be to risk substantial chilling effects on individual online behavior, because people instinctively recognize that compilations of sensitive data are dangerous to them, whether through misuse by a carrier or release to a hacker.

It might be argued that as long as the use of such information by carriers is blocked, carriers will have no incentive to retain data, and therefore such rules are unnecessary. But if incentives for collecting personal data not related to the provision of service are absent, then data retention limits will do no harm. However, such data is worth money in today’s world, large companies tend over time to seek out every possible way to make money, and there may be incentives for carriers to collect such data that we cannot now anticipate. And, meanwhile, the security risks would mount.

The Commission asks for comment on the contours of data retention rules. We think that rules should prohibit the collection of data not reasonably necessary for the provision of service, and

¹² Bruce Schneier, *Data Is a Toxic Asset*, SCHNEIER ON SECURITY, (Mar 4, 2016), https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html.

¹³ *Id.*

¹⁴ 47 U.S. Code § 222 (a)

destruction within a reasonable time of data that was once but is no longer needed for the provision of service. Data retention policies must be transparent, and scrutinized to ensure that claims of necessity under the provision of service exception (such as the spam filtering example the Commission cites) are reasonable, and that the data retention is actually related to any such purposes.

It is true that some data retention can be socially beneficial, but the potential for such benefits must be balanced against the risk that any openings will be exploited for the profit of carriers and the detriment of customers and the network overall. As with medical information, individuals' private (and, inevitably, often sensitive) communications data should not be used even for such purposes as academic research without their informed consent.

We do not believe that the application of these rules should be contingent upon the sensitivity of the particular data that is collected, but should apply to all data, because the sensitivity of data is a highly subjective and context-specific determination that is unique to each individual and his or her circumstances. Moreover, data that appears to lack sensitivity at first glance may reveal highly sensitive information about a person when subjected to algorithmic analysis by powerful software.

Requiring or rewarding the abandonment of privacy rights by customers

Customer information is worth money—and the more detailed it is, the more valuable. As a result, companies will have a continuing incentive to figure out how to induce agreement for its use from customers, creating steady pressure against the integrity of the protections the Commission creates to fulfill its statutory charge of protecting the privacy of our telecommunications networks.

One danger is that the carriers will require customers to sign away their privacy rights as a condition of service, or certain kinds of service. This should be prohibited as it would create a gaping loophole that would quickly be exploited. Another danger is that customers will be induced to give up privacy protections that under the law should be their right. That may initially take the form of seductive “special discounts” for those who agree to give up their privacy, but will quickly become equivalent to extra charges for those who wish to preserve that privacy, as the “special” and the “normal” become inverted. The result will be that the underprivileged (and disproportionately minority) population that lacks the discretionary income to devote to privacy will lose a right available for purchase by more affluent Americans. The FCC needs to include protections that prohibit carriers from forcing customers to pay extra for their privacy.

While it is true that many edge providers offer free or discounted services in exchange for violations of privacy, there are at least five distinct problems with allowing BIAS providers to go down that path. First, many consumers who use these services express discomfort with doing so, and it is unclear as argued above that the current vogue for such services will persist over the long term as the extent of privacy loss and its implications gradually sink in. Second, the provision of access to the internet occupies such a unique position in our democracy, is so crucial to the carrying out of sacred functions such as self-expression, access to information, and political organizing, that it must be treated differently than the fast-evolving swirl of online

services. Broadband internet is a common carrier for a reason. Third, if the door is allowed to open to privacy-invading terms of service, a torrent of manipulative deals and offers will appear that quickly raise knotty problems for the Commission; it would be better to draw a firm line at the outset. Fourth, the state of competition among BIAS providers (oligopolistic at best) is such that the providers have too much market power and ability to channel and coerce their customers into the terms of service they find most advantageous. And fifth, consent is often not meaningful in this context since many consumers lack a full understanding of how their data may be used and its implications. Academic research shows that most consumers do not actually read online terms of service or privacy policies, because of their complexity, length, and sheer volume,¹⁵ and that even when consumers are aware of a privacy policy's existence, they reflexively believe it will *protect against* collection and disclosure of information, not facilitate it.¹⁶

Content of communications

For years after the advent of the modern telephone network it was never possible for the carriers to listen in to the content of customers' voice calls en masse, analyze that content, and make use of that information for marketing or other purposes. That era has now arrived—such mass eavesdropping could not only be done with voice calls today, it is even easier to do with data communications over the internet. The Commission must ensure that the carriers are not permitted to do this.

Congress clearly intended to future-proof the privacy protections of § 222 of the Communications Act, for example by expanding its application from the telephone network in particular to telecommunications services in general. However, in the definition of CPNI included in the statute, Congress focused on the kind of information to which the telephone carriers had mass access through the technology of the time, and focused less on content. Nevertheless it is clear that the Commission has sufficient authority to forbid the carriers from retaining and using the content of their customers communications. This authority derives not only from the general duty of confidentiality of § 222(a), but also from other overarching authorities such as the Commission's charter under § 201(b) to require that all practices connected to the offering of a telecommunications service be "just and reasonable."

And content must be protected. It would be a strange outcome if metadata were to receive strong protection, but not content; the content of communications is just as important as metadata to the substantive privacy rights of individuals. Americans do not expect their broadband providers to be reading their electronic communications any more than they expect them to be keeping a list of their correspondents. All of the reasons why Congress charged the Commission with protecting customer information "that relates to the quantity...type, destination, location, and amount of use of a telecommunications service"¹⁷ without doubt apply to content as well.

¹⁵ See, e.g., M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1032 & n.34 (2012).

¹⁶ Joseph Turrow et al., *Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace 1* (2007), http://www.law.berkeley.edu/files/annenbergsamuelson_advertising.pdf (reporting that most people think the mere existence of a privacy policy on a website means "the site will not share my information with other websites or companies").

¹⁷ 47 U.S. Code § 222(h)(1)(a).

The Commission should make this clear despite existing laws that have some bearing on the legality of content monitoring by BIAS providers. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Wiretap Act, as amended by the Electronic Communications Privacy Act (ECPA) in 1986, prohibits unauthorized interception and disclosure of oral, wire, and electronic communications.¹⁸ But three exceptions exist under the Wiretap Act that allow ISP's to access, store, share, and use the contents of user's communications. First, a provider of "wire or electronic communication service" may "intercept, disclose, or use" a communication in the "normal course of" and as a "necessary incident to" rendering the service. Second, a provider may carry out such interceptions in "the protection of the rights or property" of that provider.¹⁹ And third, a provider may intercept electronic communications if "one of the parties to the communication has given prior consent to such interception."²⁰

But BIAS providers should be prohibited from routine eavesdropping upon the content of customer communications (whether through deep packet inspection technology or any other) even with a customer's permission. Among other things, all the people that the customer communicates with have no way of knowing about or consenting to having their half of the conversation monitored in that way. That would be a profound violation of privacy that is not permitted in other contexts. Carrier monitoring of content should only be permitted briefly in particular situations such as when necessary to provide or troubleshoot technical problems or to protect the carrier's infrastructure.

"Opt-out" and "opt-in" approval

We urge the Commission to prohibit BIAS providers from using customer data or sharing it with others, except to provide the broadband service or to offer upgrades to that service, or with specific opt-in permission from their customers limited to the data needed to provide a specific separate service. Customers' private information should not be used or shared for any other purposes without their express, affirmative, written consent. Opting in should never be presented as a requirement to obtain service, consent must be verifiable and easy for customers to revoke at any time, and carriers should be obliged to comply fully with customers' choices.

The situation in our society as a whole, and with regards to broadband service in particular, should never be, "you have no privacy unless you go out of your way to insist upon it." It should be, "your activities are private unless you consciously agree to share them."

Proponents of corporate surveillance often argue that such monitoring brings many benefits to consumers. If that is the case, then customers will not want to miss out and providers should not have a hard time convincing customers to opt in to valuable services. On the other hand, if the practices in question merely help carriers increase their profits while offering nothing to consumers except privacy invasions, then consumers will rightly decide not to opt in to that monitoring or sharing. For all the rhetoric of consumer "choice," the widespread discomfort with Web advertisers and other tracking by edge providers discussed above shows that consumers do

¹⁸ 18 U.S.C. § 2510-2522.

¹⁹ 18 U.S.C. § 2511(2)(a)(i).

²⁰ 18 U.S.C. § 2511(2)(c).

not feel these practices are increasing their choices and empowering them, but to the contrary are making them feel trapped.

Companies' continuing incentive to figure out how to induce agreement from customers to share valuable personal data brings a high likelihood that any loopholes in customer consent will be exploited, for example by gaming the definition of "affiliates" to make use of information. A clean, across-the-board opt-in rule will foreclose such attempts at manipulation, and create clarity for customers and carriers alike.

Conclusion

The ACLU strongly supports the Commission's proposal to apply the traditional privacy protections of the Communications Act to broadband internet access service, and believes that it represents a critical step in preserving the privacy of our communications infrastructure and therefore the integrity of that infrastructure. The current prevalence of privacy invasions among certain edge providers does not enjoy wide legitimacy and should not be used to justify a betrayal of legally clear, culturally deep, and historically longstanding protection for privacy in our essential communications infrastructure. The Commission should recognize that customers' economically valuable personal data will continue to exert a strong pressure on companies, who will likely be tempted to exploit every crack in the regulatory protections to increase revenues. The Commission should proceed on that assumption and enact the strongest possible protections for privacy.