Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

Comments of
Will Rinehart[1]

The proposed privacy rules[2] before the Federal Communications Commission (FCC) represent the exact wrong direction for the agency, for the industry, and for consumer protection. As noted in the rules themselves, they represent a significant shift from current policy. In sum, the FCC's privacy rules are a misfire for five primary reasons:

1. The rules would push the agency into unchartered territory, shoehorning privacy rules to meet the requirements of statute;
2. The agency doesn't have the privacy expertise to implement these rules;
3. The agency also doesn't have the institutional structure to implement these rules;
4. The FCC acknowledges that the privacy rules are not needed in order to protect consumers; and
5. Lastly, privacy regulation elsewhere has shown that serious costs will be imposed by these proposed rules, putting a heavy burden on innovation.

The result would be the most detailed and burdensome data privacy regime that has yet been devised without precedent either in the Federal Trade Commission (FTC) or the US legal structure.[3] It would conflict explicitly with longstanding principles and current privacy obligations elsewhere in the economy. It would create regulatory asymmetry, where broadband service providers would be subject to prophylactic rules, while the rest of the technology space, and indeed some of their closest competitors, would be subject to a less heavy handed case by case regime enforced by the Federal Trade Commission. In the end, the rules would result in misaligned security incentives and distorted consumer preferences, leading to less innovation on the Net, higher costs to consumers, and in the agency's own words, "competitive ripple effects." The FCC should instead forbear from

---

[1] Will Rinehart is Director of Technology and Innovation Policy at the American Action Forum.
[2] Federal Communications Commission, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0401/FCC-16-39A1.pdf.
[3] Jon Leibowitz, *Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC Docket No. 16-106*, http://apps.fcc.gov/ecfs/comment/view?id=60001910301.

applying privacy rules, and shift the burden towards Congress to resolve the gap, which would put the onus back on the FTC where it has been for decades.

1. The Privacy Rules Would Push the Commission Past its Legal Bounds

Because the FTC is exempted from bringing actions against common carriers, when the Commission reclassified Broadband Internet access service providers (BIAS) to be a Title II service, the FCC ripped from the FTC its jurisdiction over privacy, creating a mess in agency jurisdiction. Naturally, the best remedy for this problem is for the agency to forbear kicking it back to Congress to amend this part of the law, a suggestion of FTC Chairwoman Edith Ramirez, and then write into the Communications Act a provision limiting the FCC from pursuing this avenue again.[4]

This Notice of Proposed Rulemaking (NPRM) finds the FCC pushing an entirely new set of privacy rules to fill this manufactured gap, and asks for comment on how to do that legally, even though the legal basis for reclassification is still an issue before the court. One particularly odd part about this proceeding is that the agency already claims all the power it would need to enforce some sort of privacy regime, since it settled with Verizon over privacy issues using the same legal interpretation as they make in this proceeding. As TechFreedom has astutely pointed out, the only theoretical difference between formal rules and the powers that agency has already claimed comes in the realm of monetary penalties, since "the Commission cannot impose a penalty in the absence of 'fair notice of what is prohibited."[5] Yet, that didn't seem to stop the agency from imposing a $7.4 million fine in the Verizon case with formal rules. Practically, this proceeding doesn't accomplish much, other than pushing out the bounds of agency power to its extreme limits.

The agency largely cites Section 222 of the Communications Act, colloquially known as Customer Proprietary Network Information or CPNI rules, as the basis of their authority for the new rules.[6] The CPNI rules grew from a series of inquiries by the FCC in the 1970s to provide a framework for the nascent Internet technologies, and were codified in the 1996 update to the Communication Act. The CPNI sets a framework to protect consumer "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service" that "is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." What is abundantly clear from the record of enforcement, which the agency details, is that the FCC used CPNI for a limited set of enforcement actions, but the agency explicitly wants to carve out for itself a more powerful role.[7]

---

[4] Maureen K. Ohlhausen, *FTC-FCC: When is Two a Crowd?*, https://www.ftc.gov/system/files/documents/public_statements/893473/151204plispeech1.pdf.

[5] TechFreedom, *Why Is the FCC Rushing through Privacy Rules? Normal 90-Day Comment Window Wouldn't Leave Consumers Unprotected,* https://techpolicycorner.org/why-is-the-fcc-rushing-through-privacy-rules-a5ef06eb53be#.cr7edri4j.

[6] Legal Information Institute, *47 U.S. Code § 222 - Privacy of customer information,* https://www.law.cornell.edu/uscode/text/47/222.

[7] Federal Communications Commission, *Enforcement Actions (By Date)*, https://transition.fcc.gov/eb/tcd/eabydate.html.

Under this current chairman, the FCC has fundamentally shifted their understanding of CPNI, so that it now includes a broad grant of authority over privacy based not just in Section 222 but also in Section 201 and Section 706 of the Communications Act. This newer vision includes vast discretion and few limits over all privacy matter on the Internet.

This proceeding marks a grim milestone in a series of power grabs by the agency. Does the agency care about what was traditionally enforced? No. "We do not so limit ourselves here."[8] Does the FCC care that they are vastly expanding agency action beyond the mere statutory definition of CPNI? No. The law "should not be so narrowly construed."[9] This proceeding should be seen for what it is. It is yet another move in a series of worrying power grabs by the Commission, which severs it from its Congressional tether.[10]

2. The FCC Doesn't Have the Expertise to Soundly Implement these Rules

Notwithstanding the countless questions and proposals raised, the suggested rules show a clear disconnect between the FCC, on one hand, and the FTC, the Cybersecurity Framework produced by the National Institute for Standards and Technology (NIST), as well as the rest of the privacy community on the other.

The rules outline five kinds of information that the agency claims meet the definition of CPNI:

1. Service plan information, including type of service (e.g., cable, fiber, or mobile), service tier (e.g., speed), pricing, and capacity (e.g., information pertaining to data caps);
2. Geo-location data;
3. Media access control (MAC) addresses and other device identifiers that are unique for each wired or wireless device;
4. Internet Protocol (IP) addresses and domain name information; and finally
5. Internet traffic statistics.

And yet, geo-location data, MAC addresses and IP addresses aren't just "available to the carrier by the customer solely by virtue of the carrier-customer relationship," as explained in the statute. The Internet is based on protocols that share IP addresses, databases often collect MAC addresses, and apps use geo-location services to target their services.[11] In short, none of these three kinds of data actually meet the definition, as intended by the statute. So either the commission doesn't understand the technical nature of what it is regulating, or it is specifically trying to distance itself from the statute. Both are likely the case and are both reasons to reject this proposal and kick the issue back to Congress and the FTC.

---

[8] See footnote 1 at paragraph 298.
[9] Ibid at paragraph 299.
[10] Will Rinehart, *The FCC Changes The Definition Of Broadband,* http://www.americanactionforum.org/insight/fcc-changes-broadband-definition/.
[11] See footnote 2.

Part of the plan would also require broadband providers to take reasonable steps to protect consumer data, but in doing so would directly contradict the Cybersecurity Framework produced by NIST.[12] By mandating risk assessments and audits of the information types above, the rules would divert attention away from protecting information that is truly sensitive and induce the company toward compliance. It has long been recognized that companies know the risk of their systems better than regulators. Requiring specific processes and treatment of certain data means that firms cannot be adaptable to changing business models and cannot include new technologies as they become available. In short, these rules would mandate security obsolescence.

The proposal also suggests implementing a data breach notification law of the above data, even though federal laws have never passed Congress. Under the current plan, the FCC would force companies to notify consumers that their information was breached no later than 10 days after discovery. Every state except for Alabama, New Mexico, and South Dakota has a breach notification laws on the books and currently the shortest time comes from Florida at 30 days. Complex breaches take time to discover, especially if the hack was sophisticated. Even the Target breach, which took three weeks, was considered a short time frame according to privacy experts.[13] Shortening that time frame to 10 days would be disastrous.

Notification law focuses on specific data types, called personal information (PI), and mandates information disclosure when name along with another type of data is leaked. PI often includes Social Security numbers, driver's license numbers, credit card number or debit card numbers, information that uniquely identifies a person. The FCC wants to define PI broadly, so that not only are five information types above included, but countless others as well, like email addresses and online identities. For a company to comply with this law, any potential breach would have to be released before the company knew exactly what happened, and at $60 to $65 per notice, it can get quite pricey. The FCC's proposed rules are stringent and inflexible in a way that ignores current breach notification laws. The FCC should defer to state laws on this issue.

The problems continue. As the FCC explains, "BIAS providers are the most important and extensive conduits of consumer information and thus have access to very sensitive and very personal information that could threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears."[14] This is factually incorrect.

For one, countless other services are "extensive conduits of consumer information and thus have access to very sensitive and very personal information," including social networks, search engines, webmail and messaging, operating systems, mobile apps, interest based advertising, browsers, Internet video providers, and e-commerce platforms.[15] Indeed, reports project that 70 percent of

---

[12] Ibid.
[13] Kelli B. Grant, *Why did Target take so long to report the breach?*, http://www.cnbc.com/2013/12/19/why-did-target-take-so-long-to-report-the-breach.html.
[14] See footnote 1 at paragraph 2.
[15] Peter Swire, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.

the total traffic on the Internet will be encrypted by the end of this year, so ISPs will often not be able to see this sensitive information.[16] The proposal is one of the most complex in recent memory. Over 500 questions are asked, which should hardly be surprising because the FCC lacks institutional expertise.[17] Unfortunately the proposal does not seek comment on how it will affect innovation nor does it seek to understand how privacy is actually balanced by companies in practice.

Former Federal Trade Commission Chair Jon Leibowitz has noted that these rules "propos[e] regulations for broadband providers that go well beyond those imposed upon the rest of the Internet economy and which, if adopted, would undercut benefits to the very consumers it seeks to protect."[18] He further warned that caution was needed, and encouraged the agency to "take the time necessary to carefully evaluate how those rules would affect business practices."

In spite of this, the FCC administration has pushed for an expedited review, shortening the normal time to comment from 90 days to 57 days. Uncharacteristically, some of the most vocal privacy advocates cheered this narrowing of the debate.[19] In doing so, both the privacy advocates and the FCC have shown that they don't much care about getting the policy right but about getting it passed before the next election. The rampant politicization of the agency indicates that it isn't the best regulator for this important job and that it should forbear from applying privacy rules, and allow Congress to hand the regulatory power back to the FTC.

3. The FCC Doesn't Have the Institutional Structure to Soundly Implement these Rules

While the NPRM looks to current privacy practices and especially the FTC for guidance, nothing in the 147 pages suggests that the Commission appreciates what is needed at an institutional level to accomplish this job.

For one, the FTC has spent considerable resources to become the preeminent privacy regulator. It is staffed with privacy experts and economists in formalized bureaus, it has solicited feedback on proposals, organized workshops, issued staff reports, testified in front of Congress over decades, and has brought over 100 privacy and data security cases.[20] The FTC has even brought consumer protection actions against AOL, Compuserve, Prodigy. The FCC on the other hands has done none of these. It doesn't have a formalized office. It hasn't issued staff reports. That the agency chooses a formal rulemaking without first issuing a notice of inquiry or a policy statement means that it isn't much concerned with getting the policy right.

---

[16] Sandvine, *Encrypted Internet Traffic: A Global Internet Phenomena Spotlight*, https://www.sandvine.com/downloads/general/global-internet-phenomena/2016/global-internet-phenomena-spotlight-encrypted-internet-traffic.pdf.

[17] Will Rinehart, *20 Years Later, The FCC Still Needs To Align With Competition*, http://www.americanactionforum.org/insight/20-years-later-the-fcc-still-needs-to-align-with-competition/.

[18] See footnote 2.

[19] Center for Digital Democracy, et al., *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, http://apps.fcc.gov/ecfs/comment/view?id=60001657538.

[20] See footnote 3.

Second, while there are clear problems with the FTC, the agency is bound to a consumer welfare standard, which imposes some institutional demands for empiricism and has created a robust body of law around that standard. On the other hand, the FCC's public interest mandate imposes nothing in the way of empiricism because it is a mandate that is reinterpreted with every new Commission. As AAF has explained before, among the most worrying features of the public interest mandate is that it has likely slowed the incorporation of empirical analysis at the FCC.[21] Unlike the FTC, the FCC doesn't have a bureau of economic analysis even though it is a standard of every modern regulatory authority. A survey of regulatory agencies across the world found that the FCC was staffed by far more lawyers than other regulators; economists and technologists went seriously underrepresented. An FCC understaffed with economists and technologists but overstaffed with lawyers and advocates that don't acknowledge the limits of agency action will surely spell disaster for consumers.

4. The FCC Acknowledges that Privacy Rules Aren't Needed to Protect Consumers

In the second paragraph, the FCC lays out why it is pushing these new rules, saying that "consumers must be able to protect their privacy, which requires transparency, choice, and data security."[22] And yet, just a couple of paragraphs later, the FCC concedes that large broadband providers have already done extensive work in ensuring consumers are protected. Not only have broadband providers posted privacy policies, but they have also integrated into the company, "chief privacy officers, and together with their staffs and colleagues, they work to improve their companies' abilities to inform consumers of privacy practices, provide consumers with meaningful opportunities to control consumers' own data, and ward off attempts to breach the security of their broadband networks."[23] Considering that the agency is looking to exempt small carriers from the rules, all combined you have to scratch your head and wonder, didn't the FCC admit that the market is providing exactly the kinds of protections they are trying to implement?

By all measures, the FCC has failed in passing the three-part test AAF previously laid out for new regulation:[24]

1. Prove the existence of market abuse or failure by documenting actual consumer harm, following the approach set by the Federal Trade Commission;
2. Explain how current law or rules are inadequate, and show that no alternatives exist including market correctives, deregulatory efforts, or public/private partnerships to solve the market failure; and
3. Demonstrate how the benefits of regulation will outweigh the potential countervailing benefits, implementation costs, and other associated regulatory burdens.

---

[21] Ibid.
[22] See footnote 1.
[23] Ibid at paragraph 10.
[24] Will Rinehart, *A Framework To Reform FCC Competition Policy,* http://www.americanactionforum.org/research/a-framework-to-reform-fcc-competition-policy/.

Only later in the proposal does one understand the fundamental mistake, because the agency argues that this "privacy protection demonstrates that consumers need not choose between continued broadband investment and deployment, on the one hand, and protection of their privacy and data security on the other."[25] For privacy experts, the idea of a costless tradeoff is seen for the myth that it is. As Kenneth Bamberger and Deirdre Mulligan have detailed in a series of articles and in a book, implementing privacy on the ground is very different than writing it on the books.[26] What they reveal in their extensive review of actual corporate management practices is that ex post regulation by the FTC, in conjunction with privacy advocates, professionals, and market forces created a more ambiguous legal environment. In doing so, compliance with procedural measures was substituted with more substantive ones, leading companies to seek "the vindication of consumer expectations regarding the treatment of personal information." In other words, because companies know they have to protect consumers' actual experiences and not try to conform to a law did actually implement substantive protections, while in other countries the opposite was the case. While the FCC doesn't recognize it, there is a tradeoff between regulation and substantive protection.

5. The Proposed Rules Will Slow Innovation

The Commission has proposed a three-part legal regime that would regulate the five categories of data mentioned previously:

- For customer data that is used to provide broadband services, for example to ensure that a communication destined for a particular person reaches that destination, the rules will not generally limit transfer or sharing of information.
- The new rules would allow broadband providers themselves or through their affiliates to use customer information to market other communications-related services, but they would be subject to opt-out approval of the customer.
- Lastly, broadband providers will have to expressly receive an opt-in approval from their customers before it can share customer information with noncommunications-related affiliates or third parties

For one, only broadband providers will be subject to these rules, and not their counterparts who also deal with massive amounts of data. Thus, the imposition of both opt-out and opt-in rules will create a regulatory imbalance within this sector. In the US, mandates requiring companies to allow consumers opt-out or opt-in of information sharing is limited to specific sectors where Congress has determined that there is a strong case harm could come from inadvertent sharing. While there might be some cases where leaked information in concert with other types of information could be compromising to an individual, as explained above, there is nothing particularly unique about what broadband providers can access. Others often have access to this information as well.

---

[25] See footnote at paragraph 11.

[26] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2305&context=facpubs.

Moreover, companies that have integrated vertically will be split internally. Both Verizon and Comcast have both a communications related service in the form of a broadband service and non-communications service in the form of a content company. Under these rules, information sharing would be split among these activities. The FTC doesn't make such a distinction and treats affiliates as first parties when the relationship is clear to consumers.[27] Moreover, the FTC framework typically calls for an opt-out, not an opt-in because it imposes heavy costs.

Here is what an opt-in regime for those non-communications-related services would look like in practice. Sprint recently inked a deal with Amazon to offer their customers the Amazon Prime service.[28] Under the proposed rules, Sprint would have to get explicit approval from every customer *before* it could tell them about this deal. AT&T is betting big on home automation services. By all accounts, this change in policy would limit them from cross company deals and telling consumers about new products. And what about the growing Internet of Things market? Would companies in this market also be precluded from sharing information across its entities? Considering how the rules have been proposed, this is likely, which would impose a huge unseen cost to innovation in this space.

Opt-in regimes present three big hurdles for consumers as decision makers. First, consumers have substantially less information about decisions they make. Before any additional service can be provided by the ISP, consumers will have to imagine all of the potential benefits, which will be difficult if not impossible. Second, consumers will think that that defaults are suggestions by the company. In other words, they will assume that it is a recommended action, even though they are mandated by the government. Lastly, these defaults will become the status quo. Any further change from this baseline will require significant effort by the ISP and will be understood by the decision maker as a trade-off, as psychologists have found.

Opt-in defaults show markedly lower participation rates to opt-out defaults even though the good or service is exactly the same. The classic example is organ donation. Although there is widespread approval of organ donation, around 85 percent of Americans want to be donors, only about 28 percent actually sign their card. Some countries automatically enroll everyone for organ donation and then allow for opting out, which results in participation rates of 85 percent and higher. Below is a compendium of studies testing these defaults. Even though consumer's options and protections are the same, the default changes dramatically participation rates.

---

[27] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[28] Sprint, *Amazon Prime Offer*, https://www.sprint.com/landings/amazon-prime/index.html.

Subject Area	Opt-In Participation Rate	Opt-Out Participation Rate
An on-line survey asking participants if they want to be contacted further about health surveys[29]	48.2 percent	96.3 percent
Organ donation[30]	Denmark 4.25 percent	Austria 99.98 percent
	Netherlands 27.5 percent	Belgium 98 percent
	United Kingdom 17.2 percent	France 99.9 percent
	Germany 12 percent	Hungary 99.9 percent
		Poland 99.5 percent
		Portugal 99.6 percent
		Sweden 85.9 percent
401(k) enrollment[31]	37 percent	85.9 percent

The FCC has previously foisted these rules on the industry before, losing in federal court and in the court of opinion.[32] In a court case with US West, a telephone company that is now part of CenturyLink, it was revealed that obtaining permission cost between $21 and $34 per consumer. By their own internal calculations, US West had to make 4.8 calls to each customer household before they reached an adult who could grant consent to share information. In one-third of households called, U.S. West never reached the customer. Altogether, customers received more calls from the opt-in regime than in an opt-out system even though many weren't able to enjoy the benefits of new services.

In other industries where opt-in regimes have been imposed, studies have found higher costs and slowed innovation. A 2000 Ernst & Young study of financial institutions found that these mandates cost the entire industry $56 billion.[33] For charities, the cost of compliance with an opt-in privacy law would have been nearly 21% of their total revenue.[34] In Europe, the implementation of restriction information sharing rules decreased the efficacy of advertising by 65 percent relative to

---

[29] Eric J Johnson, Steven Bellman, and Gerald L. Lohse, *Defaults, Framing and Privacy: Why Opting In-Opting Out,* https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf.
[30] Eric J. Johnson & Daniel Goldstein, *Do Defaults Save Lives?*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.173.2319&rep=rep1&type=pdf.
[31] Betty Joyce Nash, *Opt in or Opt out: Automatic enrollment increases 401(k) participation*, https://www.richmondfed.org/~/media/richmondfedorg/publications/research/region_focus/2007/winter/pdf/feature2.pdf.
[32] Julie Tuan, *U.S. West, Inc. v. FCC*, http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1276&context=btlj.
[33] Ernest & Young, *Customer Benefits from Current Information Sharing by Financial Service Companies*, http://www.netcaucus.org/books/privacy2001/pdf/ernstyoungreport.pdf.
[34] Fred Cate, *The Privacy Problem A broader view of information privacy and the costs and consequences of protecting it*, http://www.firstamendmentcenter.org/madison/wp-content/uploads/2011/03/FirstReport.privacyproblem.pdf.

the rest of the world, cutting off the lifeblood of Internet startups.[35] The cost of privacy regulation is one of the reasons why Europe lags in startups. And the FCC wants to pile on those costs.

In practice, the new rules would implement soft paternalism, which has been a hallmark of this administration. Even though no additional privacy protection would be afforded, the rules would result in distorted preferences, leading to less innovation on the Net and higher costs to consumers.

Conclusion

In spite of the overwhelming evidence of harm, the FCC is determined to apply new burdens on ISPs. As currently written, they fail for five reasons. One, the rules would further the agency's unchecked power into unchartered territory. Two, the agency doesn't have the expertise to soundly implement these rules so that they don't harm consumers. Third, the agency doesn't have the right institutional structure to completely understand the privacy space. Fourth, the agency actually acknowledges that the privacy rules are not needed and that consumers are getting protection via market incentives and the FTC. And lastly, the when the rules have been applied elsewhere they are shown to be costly to consumers and innovation without any additional privacy protections.

The costs of this plan are myriad, hidden in the default that compels an inefficient default and in an agency groping for power. And yet, the upsides, which the FCC has failed to show, are few. For those of us who haven't given up on American innovation and who care about consumers, these proposed rules represent the absolute wrong way forward. The FCC should forbear from applying these rules and kick the issue back to Congress so that the FTC can again take up the mantle of privacy enforcer for the United States. Anything less will be a disaster.

---

[35] Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Online Advertising*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.