Remarks of FCC Commissioner Michael O'Rielly
Before the Catholic University Columbus School of Law Technology Institute Panel Entitled
"Protecting Consumer Privacy and Promoting Innovation in the Internet Era"
November 2, 2016

Thank you for that very kind introduction. I appreciate the opportunity to be the kickoff speaker for this panel on an important topic just considered by the Federal Communications Commission, or as it is known to many, The Catholic Law School Annex. Not surprising, many of the graduates of this institution play key roles at the Commission and are integrally involved in the formation of communications policy. They are in the know, pulling the policy levers and influencing outcomes. As a Commissioner in the minority often left out of the loop, it makes me extremely jealous.

Turning to the topic at hand, as many of you know, the Commission recently adopted rules that impose new burdens on supposed "rogue" Internet Service Providers under the guise of protecting consumer privacy.[1] The three-to-two vote fell along party lines, placing me in the non-winning camp once again. While the text of the item is not available at the moment – a flaw in the Commission procedures – I am free to express my thoughts and views on the item and the topic as a whole.

Let me set the stage for our discussion by highlighting the true purposes of data collection and analytics in this sphere. For those that have examined the issue, as I believe I have, you come to realize that there are three broad reasons why commercial companies collect and use consumer's data, either offline or online. The first is to market additional or new products or services to their customers or to sell the information to others to do the same. From Internet banner ads to store mailings to grocery store coupons, the ultimate goal is to reach the consumer to make a sale. The more data collected, the greater the chance to target the pertinent material or merchandise to the right people (i.e., those truly interested), minimizing the failure costs for the company and the annoyance factor for uninterested consumers. The second function is to improve the functionality, profit efficiency, or other aspects of the company's operations. By analyzing the requisite data sets, companies can detect how to improve their offerings or the means they use to offer products or services. In other words, it is a chance to examine the point, or points, at which a company's offerings can better meet the demand of consumers in the future or show where they are going wrong. In addition, companies collecting data may sell such information to other companies for the same purpose. The last reason for private companies to collect such consumer data is to either comply with legal or law enforcement requirements or to sell the information to government entities. Sometimes this is done begrudgingly and other times it results business opportunities.

Even for the most privacy conscious person, the first two purposes should not produce the same level of concern as the last. Admittedly, there may be an added nuisance factor of receiving additional tailored ads from companies seeking to more effectively target them for sales. On the other hand, better targeted ads and more proficient companies can serve to meet more consumer needs. While such advertising may help increase demand for those trying to sell the specific good or service featured in the ad materials, it also dramatically reduces the cost of products and services for consumers. For instance, just imagine the cost of local television broadcasting or Google's applications without advertising. Far from being a dirty word, it is an honorable profession harnessing some of nation's most creative people and is a key ingredient in American commerce. More importantly, we all should

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, FCC 16-148 (rel. Nov. 2, 2016) (*Privacy Order*).

acknowledge that legitimate advertising (i.e., non-deceptive) is a societal good that is also protected by the U.S. Constitution. Those seeking to squash it, attack it or restrict it had best do more homework before making outrageous statements or seeking to undermine it. You will get little support in doing so from me.

On the other hand, I would argue that the American people should be most concerned about how data is collected, compiled, analyzed and shared with national security or law enforcement entities. In the wrong hands or used for the wrong purposes, such data could ultimately be used to lessen individual liberty and/or private property rights. Combined with mechanisms to force compliance, the use of data could be abused or manipulated in a harmful way. But that gets far afield from the authority of the FCC, and I have to defer to Congress on whether or not to impose limitations on the sharing of such information with government representatives.

Setting the law enforcement debate aside, I think it is important to understand the charge of a Commissioner. My first function is to determine whether or not there is a problem that needs to be solved or resolved. When determining whether to dictate government interference in the private marketplace, you had better be sure that there is data-driven evidence of market failure and not just hypothetical or potential harm. New FCC regulations impose burdens on providers that affect their decision-making in terms of products or services offered, markets entered or withdrawn, people employed or to be let go, customers to be served or abandoned and many other factors. It can dramatically change the direction of the marketplace.

Assuming a problem or issue exists, I next turn to whether and, if so, to what extent the Commission has authority to take some action. To provide guidance and boundaries, Congress governs our activities via the Communications Act of 1934, a couple of other statutes and close oversight. To be clear, there may be areas where I might agree action is warranted but is, in fact, not permitted by law. My role is not to charge ahead based on my personal interests and beliefs. Instead, I have the right and, in some instances, the obligation to inform Congress of my views in a suitable way and then let our duly elected representatives make decisions as they see fit.

With that understanding, let's return to the recent FCC item, which is focused solely on limiting the ability of one set of Internet companies – broadband providers – to collect and use consumer data, to the extent that they actually collect and/or use it. How the Commission arrived at last week's action was fairly predictable. By reclassifying broadband Internet access service as a telecommunications service under Title II, as part of its misguided campaign to impose "Net Neutrality" rules, the FCC, as a result, usurped part of the Federal Trade Commission's role in overseeing broadband privacy. Not content to inherit a system that, by almost all accounts, was working quite well to protect consumers, the FCC dismissed the privacy structure developed and implemented, through extensive precedent, by the FTC over a number of years. In its place, the Commission explored radical alternatives, finally settling on an item that establishes new and unique restrictions on the collection and use of information by Internet Service Providers (ISPs).

From my perspective, the biggest substantive areas of concern are (1) the ill-conceived definition of sensitive information, which includes web browsing history and application usage and thus requires consumer opt-in mechanisms; (2) the unreasonable limitations on first-party marketing; and (3) the effective establishment of a new Commission regime to review consumer privacy trades.

Let me walk you through my objections to the Commission's inappropriate action:

1. No Existing Problem

Fundamentally, I disagree with the notion that there is an existing problem worthy of Commission action. There is very little real evidence in the record that ISPs have or are planning to dissect the consumer traffic that they carry to a degree that would result in consumer harm. To the contrary, the record shows that a substantial percentage of Internet traffic is encrypted, with that number increasing in the near term. That means that ISPs, certainly smaller and medium companies, have little to no direct access to the wealth of consumer data and information considered valuable. At the same time, consumers use multiple platforms to access the Internet, significantly undermining the Commission's claims that broadband providers have unique or unparalleled access to customers and their information.

Even if you ignore these facts to support the need for new rules, the prudent thing would have been to adopt the FTC approach, not to illogically capture web browsing history or app usage that by their very nature are not intrinsically important, much less private. As with the FTC's model, if use of the web or an application generates sensitive data, such as health or financial information, then it is already covered by other existing categories. There is no need to be over inclusive in the definition's scope.

2. No Legal Authority

The Commission's attempt to fit broadband into current law, specifically section 222, is fundamentally flawed. The plain language of the statute speaks in terms of telephone service. And no other section is remotely relevant to authorize FCC action. Accordingly, in its effort to shoehorn broadband into this regime, the Commission is forced to ignore or explain away language that clearly contradicts its position, regulate by analogy, or simply create new obligations out of thin air. And in that, they did a poor job.

3. Undermines Consumer Expectations and Creates Confusion

The FCC claims that, in moving to a sensitivity-based framework, the rules will be "more properly calibrated to customer and business expectations."[2] But requiring opt-in notice for web browsing history and application usage data is a significant departure from the FTC approach, which is the basis for current consumer and business expectations. While this has been in effect, businesses have been able to "provide great value to consumers in the form of discounts, convenient features, and other new and innovative services."[3] Requiring opt-in consent for these categories will destroy that value and upend years of settled expectations, burdening rather than benefitting, most users.

Additionally, consumers will receive new privacy notices from their broadband providers asking them to opt in for certain practices. If they do not opt in, but continue to see advertisements based on their web browsing and application usage, some will understandably assume that their broadband providers are violating their privacy policies when, in fact, the ads originate from third parties not subject to FCC rules.

---

[2] *Privacy Order* at para. 173.

[3] Letter from Michelle R. Rosenthal, T-Mobile USA Inc., to Marlene Dortch, FCC, WC Docket No. 16-106, at 2 (filed Oct. 14, 2016).

4. Enacts Harmful Restrictions

The Commission's action limits inferred consent to only first party marketing within a service category, as well as the marketing of consumer equipment and "communications services commonly bundled together with the subscriber's telecommunications service."[4] Here again, there is no rational reason to place undue restrictions on broadband providers. Instead, we should have extended inferred consent to the marketing of products and services offered by providers and affiliates as long as the affiliated relationship is clear to consumers. As the record demonstrated, consumers expect to receive information from their providers about new products, services, and discounts. In addition, if broadband providers "cannot market new products and services on the same terms as online companies – or even other brick and mortar businesses – there will be less incentive to invest and develop new services."[5]

In addition, the Commission installed a case-by-case approach to review and possibly reject consumer privacy trades, the willing exchange of private information by consumers to providers for service features or functions. These types of consumer financial incentives are offered every day in the real world, and now ISPs will need to obtain a blessing from an agency that has no privacy experience. The end result is that broadband providers will be reluctant to extend, and may even forgo, valuable offers and discounts that consumers would want for fear that they will fall into another zero-rating style abyss.

5. Ineffective & Costly

The ultimate absurdity of these new rules is that broadband providers remain free to purchase and use the information they need from other Internet companies, including edge providers, because these other companies, not covered by the rules, will continue to operate under the FTC's opt-out regime. Therefore, all that the FCC has really done is to raise the transaction costs, requiring consumers to pay more for heightened privacy rules that they never asked for.

* * *

Hopefully, I've provided a sufficient platform or enough material for the subsequent panel to debate these issues in greater detail. Before that occurs, I promised that I would take some questions from the audience.

So thank you for your attentiveness and I'll open the floor to the first question.

[4] *Privacy Order* at para. 204.

[5] Letter from Jennifer Hightower, Cox Communications Inc., to Marlene Dortch, FCC, WC Docket No. 16-106, at 3 (filed Oct. 20, 2016).