

July 26, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other
Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

On July 22, 2016, Harold Feld and Dallas Harris of Public Knowledge met with Melissa Kirkel, Heather Hendrickson, Sherwin Siy, David Brody, Brian Hurley, and Bakari Middleton of the Wireless Competition Bureau, with regard to the above captioned proceeding. Public Knowledge discussed the proper analysis of harm in the context of anonymized data, infeasibility of employing a sensitive vs. non-sensitive approach, and the Commission's previous determination that PII is CPNI.

Nature of Harm Identified By The Statute

Many argue that when information is anonymized there is no harm to the consumer and therefore, no consent should be required to use anonymized information. This mistakes the purpose of Section 222.¹ As explained in the Senate Conference Report, Section 222 as proposed by the House offered 3 protections to consumers: “(1) the right of consumers to know the specific information that is collected about them; (2) the right of consumers to have proper notice that such information is being used for other purposes; and, (3) the right of consumers *to stop the reuse or sale of the information.*”² In describing the “compromise” reached between privacy and competition, the Conference Report further explained that “use of CPNI is limited, except as provided by law *or with the approval of the customer.*”³ This emphasis on placing the control in the hands of the customer, not merely to prevent shielding the information from third parties, is consistent both with the strict limitations on use of the information by the carriers (regardless of whether they reveal the information). Likewise, it is consistent with all previous privacy statutes included in the Communications Act, which emphasize the control of the subscriber or customer over the information.⁴

This is very different from the jurisdiction conferred by Congress on the Federal Trade Commission (FTC). The FTC's general privacy jurisdiction derives not from a

¹ See 47 U.S.C. § 222.

² Telecommunications Act of 1996, S. Rep. No. 104-230 at 204 (1996) (Conference Report) (emphasis added).

³ *Id.* at 205 (emphasis added).

⁴ See 47 U.S.C. §§338(i); 551; 605.

specific privacy statute (although some specific statutory provisions further enhance the FTC's privacy jurisdiction), but as an interpretation of its general consumer protection authority under Section 5, and bounded by the express limitations of 5(n).⁵ While the FCC should respect the experience and guidance of its sister agency, it must also respect the explicit direction of Congress, as evidenced by over 90 years of consistent statutory evolution, to regard the privacy of communications as uniquely sacrosanct.

In examining Congresses' actions, it is clear that Congress has as its goal, with regard to communications specifically, the idea that the consumer should be in control of their information. For various reasons discussed in our white paper, it is clear that the goal of Section 222 is not merely to avert a negative harm of embarrassment or exposure of information to third parties, but a general desire to ensure that when a subscriber sends a communications transmission, that the transmission is not used in anyway utilized by the carrier for its own gain. Section 705 has this restriction on carriers and any third party that intercepts those communications.⁶

The Cable Privacy Act is even more specific. In its liquidate damages clause, the CPA values the failure to disclose collection, use, or use without appropriate consent at \$100/day.⁷ In the context of Section 222, while there is no liquidated damage clause, the fact that Congress allows subscribers to direct disclosure of information to any third party, while simultaneously refusing to allow the carrier to use information except under certain limited exceptions, all point to a long and sustained history that the purpose of the statute is to put consumer in control of information, rather than just protect from accidental disclosure.⁸

This interpretation is further bolstered by the fact that all previous privacy acts are explicitly still in effect and should be used in combination with sec 222. Therefore, when the Commission examines the harm, it is importance to recognize there is a critical difference between what Congress has directed the FCC to do and what the FTC does. The FTC operates under a general consumer protection statute that is not specific to privacy and has not made a separate distinction with regard to violation of persons privacy or information as distinct from any other form of economic harm that it finds violates Section 5. For the Commission, Congress has made a very clear declaration.

If the Commission agrees with the analysis of the harm and that one goal of Section 222 is to maximize consumer control, then anonymization is no help. Anonymization would still convey a windfall to the carrier at the expense of consumer control of the information in a way that Congress did not intend.

⁵ See 15 U.S.C. § 45 (n).

⁶ 47 U.S.C. § 605 (1982) (redesignated as § 705(a) in Cable Communications Policy Act of 1984, Pub. L. No. 98-549, § 705(a), 98 Stat, 2779, 2804 (1984)).

⁷ See 47 U.S.C. § 551(f)(2)(A).

⁸ See 47 U.S.C. § 222(c)(2).

There is also competition argument against anonymization. Congress, in promoting competition, did not intend to allow carriers to cross subsidize their other potential businesses with the information that they obtain as carriers in the course of carrying out their Title II telecommunications responsibilities. The general pro competitive purpose of 222(a) and 222(b) is served by not allowing carries to expand their other business lines through the use of information that they collect in provision of telecommunication services. For this reason, the Commission should not permit anonymization without first obtaining meaningful consumer consent.

FTC Staff Comments - Sensitivity approach

As noted above, the statutory frameworks of the FTC and FCC are different. While distinguishing between sensitive and non-sensitive data makes sense within the context of the FTC, where they are working from a general consumer protection statute under which they are required to measure the nature and extent of the harm pursuant to Section 5(n), the Commission has a different obligation. Moreover, it is difficult, maybe impossible, for carriers to distinguish between sensitive and non-sensitive without actually looking at and assessing the information to make that distinction.

Even under the FTCs structure, people acknowledge that things like search queries can reveal sensitive information. Communications that are directed to medical facilities, financial institutions, government agencies that provide assistance, or criminal defense attorneys are all activities that are regarded as sensitive and it is becoming increasingly difficult to know whether traffic is sensitive or non-sensitive. Therefore, in compliance with a framework where sensitive information is protected, the only way to protect the most sensitive information is to assume that everything is sensitive. Once a carrier tries to distinguish between sensitive and on-sensitive information, it will invariably expose some information that is sensitive in a way that presumed it was non-sensitive.

Harmonization

The Commission has additional privacy statutes on its books that govern. One of which is Section 705, which refers directly to the nature of the content and which the Commission has considered in the past with regards to its Google Fi decision. The other is Section 551, and it companion statue Section 338(i), which by its terms, applies not merely to the actual cable service, but also to any other service that is offered through any portion of the cable system, which is defined as any communication by wire and wireless.⁹ Furthermore 551 explicitly states that it does not displace any other remedies that may also apply.¹⁰

These sections would apply to a limited class of ISPs, those that also offer a cable service. Thus, there is a class of providers who are covered by 551, while others are not.

⁹ See 47 U.S.C. §§338(i); 551.

¹⁰ See 47 U.S.C. §551(f).

This would be an unfortunate arbitrary distinction. Therefore, for the purposes of maintaining consistency and avoiding consumer confusion, the Commission should apply the framework of 551 to 222. The best policy is to conform Section 222 to Section 551, so that all carriers are covered. Because the statutory structure is designed to work together, consumer privacy will not be weakened. Additional protections from 551 can be mapped on to 222. The best way is to make these provisions cumulative the same way that 705 is cumulative.

PII as CPNI

As a legal matter, there is a 2007 Commission order saying that PII is CPNI.¹¹ If the Commission wants to reject its previous interpretation than it needs to do more than it did in the NPRM, otherwise there is an arbitrary and capricious change. The Commission can not simply ignore its previous determination.

In accordance with Section 1.1206(b) of the Commission's rules, this letter is being filed with your office. If you have any further questions, please contact me at (202) 861-0020.

Respectfully submitted,

/s/ Dallas Harris

Policy Fellow
Public Knowledge
1818 N St., NW
Suite 410
Washington, D.C. 20036
(202) 861-0020

cc: Melissa Kirkel
Heather Hendrickson
Sherwin Siy
David Brody
Brian Hurley
Bakari Middleton

¹¹ *In re* Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927, n.2 (Apr. 2, 2007) (Report and Order and Further Notice of Proposed Rulemaking).