Prepared Statement of

The Federal Trade Commission

Before the

United States Senate

Committee on the Judiciary

On

Reforming the Electronic Communications Privacy Act

Washington, DC

September 16, 2015

Chairman Grassley, Ranking Member Leahy, and Members of the Committee, I am Dan Salsburg, the Chief Counsel in the Office of Technology, Research and Investigation, in the Bureau of Consumer Protection at the Federal Trade Commission ("Commission" or "FTC").[1] I appreciate the opportunity to appear before you today to discuss the FTC's work and how proposals to amend the Electronic Communications Privacy Act ("ECPA")[2] could impact the Commission's civil law enforcement mission.

I. FTC Background

The FTC is an independent agency with an important dual mission to protect consumers and promote competition. The FTC is the only federal agency with jurisdiction to protect consumers and maintain competition in broad sectors of the economy. Although the Commission has important education, research, and advocacy functions, it is first and foremost a civil law enforcement agency. The agency enforces laws that prohibit business practices that are anticompetitive, deceptive, or unfair to consumers, and seeks to do so without impeding legitimate business activity.[3]

The impact of the FTC's consumer protection work is significant. Between July 2013 and June 2015 alone, the FTC returned over $154 million to consumers and sent over $50 million in civil penalties to the Department of Treasury. The Commission's consumer protection enforcement actions cover a broad range of activities, including fraud. For example, in recent years, the FTC's actions have: (1) stopped fraudsters' efforts to collect "phantom" debts from

[1] The written statement represents the views of the Federal Trade Commission. Commissioner Brill issued a concurring statement with respect to Part II.C. The oral presentation and responses to questions reflect the views of the witness, and do not necessarily reflect the views of the Commission or any Commissioner.

[2] 18 U.S.C. § 2701 *et seq.*

[3] The FTC has broad law enforcement responsibilities under the Federal Trade Commission Act, 15 U.S.C. § 41 *et seq.*, and enforces a wide variety of other laws ranging from the Clayton Act to the Fair Credit Reporting Act. In total, the Commission has enforcement or administrative responsibilities under more than 70 laws. *See* https://www.ftc.gov/enforcement/statutes.

financially strapped consumers that the consumers did not actually owe;[4] (2) taken aggressive enforcement actions to stop illegal robocalls;[5] (3) sued companies that made false or unsubstantiated health claims;[6] and (4) stopped foreclosure rescue scams and deceptive payday lending practices.[7]

In bringing these actions, we rely heavily on our ability to conduct thorough investigations of companies' business practices. Targets of FTC enforcement actions

---

[4] *See, e.g.*, *FTC v. K.I.P., LLC*, No. 1:15-cv-02985 (N.D. Ill. Apr. 6, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3048/kip-llc-payday-loan-recovery-group; *FTC v. 4 Star Resolution, LLC*, No. 1:15-cv-0112-WMS (W.D.N.Y. Feb. 9, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3202/4-star-resolution-llc.

[5] *See, e.g.*, *FTC v. Caribbean Cruise Line, Inc. et al.*, No. 0:15-cv-60423 (S.D. Fla. Mar. 4, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3196/caribbean-cruise-line-inc; *FTC v. Worldwide Info Servs., Inc.*, No. 6:14-cv-8-ORL-28DAB (M.D. Fla. Nov. 13, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3175/worldwide-info-services-inc; *FTC v. All Us Marketing LLC*, No. 6:15CV1016-0RL-28GJK (M.D. Fla. June 29, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3256/all-us-marketing-llc-formerly-known-payless-solutions-llc; *FTC v. Lifewatch, Inc.*, No. 1:15-cv-05781 (N.D. Ill. June 30, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3123/lifewatch-inc.

[6] *See, e.g.*, *FTC v. Lunada Biomedical, Inc.*, No. 2:15-cv-03380-MWF (PLAx) (C.D. Cal. filed May 12, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3067/lunada-biomedical-inc; *FTC v. Leanspa, LLC*, No. 311-cv-01715 (D. Conn. Apr. 6, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1123135/leanspa-llc-et-al; *FTC v. New Consumer Solutions LLC et al.*, No. 15-C-1614 (N.D. Ill. filed Feb. 23, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3210/new-consumer-solutions-llc-mole-detective. Commissioner Ohlhausen voted against issuing the initial complaint and accepting the related settlement orders and proposed consent agreement in this matter. *See* Dissenting Statements of Commissioner Ohlhausen, *FTC v. Lasarow* (August 13, 2015), *available at* https://www.ftc.gov/public-statements/2015/08/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-ftc-v-lasarow and https://www.ftc.gov/public-statements/2015/02/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-health; *FTC v. NourishLife, LLC*, No. 1:15-cv-00093 (N.D. Ill. filed Jan. 7, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3152/nourishlife-llc; *FTC v. NPB Advertising, Inc.*, No. 8:14-cv-0155-SDM-TGW (M.D. Fla. filed May 15, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3116/npb-advertising-inc-et-al; *Health Discovery Corp.*, No. C-4516 (Mar. 13, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3211/health-discovery-corporation-melapp-matter; *FTC v. Genesis Today, Inc.*, No. 1:15-cv-00062 (W.D. Tex. filed Jan. 26, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3283/genesis-today-pure-health-lindsey-duncan. Commissioner Ohlhausen voted against accepting the proposed consent agreement. *See* Dissenting Statement of Commissioners Ohlhausen and Wright, *FTC v. Genesis Today, Inc.* (January 26, 2015), *available at* https://www.ftc.gov/public-statements/2015/01/dissenting-statement-commissioners-maureen-k-ohlhausen-joshua-d-wright.

[7] *See, e.g.*, *FTC v. Sameer Lakhany*, No. 8:12-cv-00337-CJC-JPR (C.D. Cal. Apr. 29, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3136/lakhany-sameer-credit-shop-llc-fidelity-legal-services-llc; *FTC v. C.C. Enterprises, Inc.*, No. 8:15-cv-00585-CJC-JPR (C.D. Cal. Apr. 16, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3136-x120014/householdrelief; *FTC v. Wealth Educators Inc.*, No. cv15-2357 (C.D. Cal. Apr. 10, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1523004/wealth-educators-inc.

increasingly use electronic media and the Internet to reach consumers, transact business, and retain records. Although the Commission currently does not seek content of e-mails and other electronic communications covered by ECPA from ECPA service providers, we believe that in the future, as more electronic communication moves to the cloud, the effectiveness of our fraud prevention program may be hampered if proposed legislation is not appropriately modified.

II. FTC Views on ECPA Legislative Proposals

The FTC supports the objectives of ECPA reform. Technology has evolved considerably since ECPA's passage in 1986, transforming the way consumers and businesses function. The FTC appreciates Congress's efforts to update ECPA to account for these technological advances and to protect consumers' privacy. And, the FTC appreciates the Committee's continued interest in hearing the agency's views on current ECPA reform proposals.

As a civil law enforcement agency, the FTC is concerned that recent proposals could impede its ability to obtain certain information from ECPA service providers in future cases. Under current law, the Commission could compel an ECPA service provider to produce a customer or subscriber's content with notice or delayed notice to the customer or subscriber under 18 U.S.C. Section 2703(b)(1)(B). The Sixth Circuit, in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), however, held that the Fourth Amendment bars warrantless access to email content held by an ECPA service provider. We currently forebear from employing the authority under 2703(b)(1)(B) to compel production of a customer or subscriber's content. Under recent legislative proposals, however, to compel content from an ECPA service provider, the government would have to obtain a criminal warrant, which is not available to the FTC. The proposals would require a warrant for content even when it is previously public commercial content advertising or promoting a product or service or the customer or subscriber has consented

to the provider releasing the content to the FTC. The proposals also would prohibit agencies such as the FTC from obtaining content when the customer or subscriber is a scam artist who refuses to produce the content to civil law enforcement. As a result, these proposals appear to prohibit civil law enforcement from compelling the content of electronic communications from an ECPA service provider under all circumstances.

The Commission believes that Congress can and should modernize ECPA in order to protect customer or subscriber's privacy interests in electronic communications while also ensuring the effectiveness of civil law enforcement agencies by authorizing such agencies to: (1) obtain previously public commercial content that advertises or promotes a product or service, such as websites and marketing materials; (2) compel an ECPA service provider to disclose content with the customer or subscriber's consent; and (3) when efforts to obtain information directly from a target fail, seek a court order compelling the provider to produce electronic content.

A. Law Enforcement Access to Previously Public Commercial Content that Advertises or Promotes a Product or Service

Previously public commercial content that advertises or promotes a product or service is critical to many FTC investigations. Indeed, most of the agency's consumer protection investigations involve advertising or other marketing claims made through electronic media. These deceptive claims may appear on the companies' websites or classified ad sites. In many instances, especially fraud cases, the scam artists change websites and electronic marketing materials frequently. When Commission staff investigates complaints about a website, the website currently viewable to the public may be different from the one about which consumers

complained. In other instances, the marketing materials may no longer be readily available due to an ECPA service provider's policy.[8]

Where the target is a fraudulent marketer, obtaining the advertisements through a civil investigative demand ("CID") to the marketer is often not a viable option for several reasons. First, the marketer may have no incentive to cooperate with the request. It may claim that it no longer has, or never itself retained, a copy. Or, it may simply deny that it ever posted the material. Second, any attempt to contact the marketer may cause it to flee, destroy evidence, or hide assets. In these circumstances, when a marketer refuses to cooperate or is unavailable, it is essential that the Commission retain the ability to use other appropriate mechanisms to obtain the information. If legislation impedes the Commission's ability to do so, it would frustrate the agency's ability to obtain evidence against the marketer and obtain relief for consumers.

Accordingly, the Commission is concerned that its robust anti-fraud program will suffer if copies of previously public commercial content that advertises or promotes a product or service cannot be obtained directly from the service provider. Under current law, Commission staff can work with ECPA service providers to obtain such previously public content in certain circumstances.[9] Without further clarification to recent legislative proposals, however, updates to ECPA would appear to prevent the FTC from compelling ECPA service providers to produce such previously public material.[10] Commission staff might then be unable to obtain

[8] For instance, on some bulletin boards, postings expire automatically, but copies may be maintained by the service provider.

[9] The Commission can compel an ECPA service provider to produce a customer's previously public commercial content that advertises or promotes a product or service so long as the provider is maintaining a copy for an independent business reason, rather than solely for the subscriber. Cf. 18 U.S.C. § 2703(b)(2)(B) (covering content held "solely for the purpose of providing storage or computer processing services to such subscriber or customer. . .").

[10] The Commission does not believe that all previously public content should be exempt from ECPA. But, a marketer has no reasonable expectation of privacy in its previously public commercial content that advertises or promotes a product or service.

advertisements that ran on a social media site from the site operator, or old versions of web sites from a scam's web site host.

Consequently, we urge Congress to ensure that any legislation updating ECPA preserve the ability to obtain previously public commercial content that advertises or promotes a product or service. This would enable the Commission to obtain such commercial content -- a narrow, well-defined category of content. At the same time, because such materials are purely commercial and were affirmatively published by a target, the target does not have a reasonable expectation of privacy in them with respect to law enforcement access.

B. Law Enforcement Access to Contents of Records with the Customer or Subscriber's Consent

Proposed amendments to ECPA permit civil law enforcement agencies to require an ECPA service provider to produce non-content information "pertaining to" the subscriber, if the customer or subscriber has consented. Under these proposals, however, this authority does not extend to the "content" of any other records of the customer or subscriber, including its business records, Web pages, or other stored communications, even if the customer or subscriber has consented to disclosure.[11]

As cloud computing becomes more widespread, it is increasingly important for a civil law enforcement agency to be able to compel an ECPA service provider to disclose such electronic content with the customer's consent. For example, a defendant may want to authorize the FTC to obtain documents directly from its cloud computing account, if the records are voluminous, or the defendant's only copies of the records are maintained on that service. Indeed,

[11] Under current ECPA, there is no separate provision that permits a civil agency to demand content from a provider when it has the consent of the customer or subscriber. Instead, the law's general provisions regarding government access to content would apply. *See* 18 U.S.C. § 2703.

ECPA already permits a service provider to divulge such content voluntarily with the customer or subscriber's consent (and this provision is not affected by proposed changes to ECPA).[12] Under current legislative proposals, however, even if the customer or subscriber has consented, the agency could not compel the cloud computing service to release that customer or subscriber's content. This disparity -- allowing ECPA service providers to disclose content voluntarily if the customer or subscriber consents, but denying law enforcement agencies the authority to compel such disclosures -- enables providers to deny the effect of a customer or subscriber's consent. Thus, the Commission recommends that the Committee ensure that civil law enforcement agencies have the authority to compel ECPA service providers to produce electronic content if the customer or subscriber has consented to its production.

C. Civil Law Enforcement Access to Content That Cannot Be Obtained from a Target

Although we do not currently obtain subscriber content from ECPA service providers pursuant to section 2703(b)(1)(B), we believe that recent legislative proposals requiring the use of a criminal warrant to obtain content from an ECPA service provider could create some obstacles in future *civil* law enforcement cases, including those against fly-by-night scammers and especially those based abroad, as well as cases against targets that refuse to respond to the agency's CIDs or discovery requests. Under these proposals, targets could simply refuse to produce content, and the FTC would be left with limited ability to obtain it. The Commission therefore suggests that Congress consider providing a judicial mechanism that would authorize the Commission to seek a court order directing the provider to produce the content if the Commission establishes it has sought to compel it directly from the target, but the target has failed to produce it.

[12] *See* 18 U.S.C. § 2702(b)(3).

III. Conclusion

Thank you for giving the Commission an opportunity to describe the important work of the agency, the critical importance of electronic communications in our investigations, and the ways in which proposed updates to ECPA, while extremely important, could hinder our law enforcement actions. The FTC looks forward to working with this Committee to address the Commission's concerns as legislation advances.