

financially

that actually owe;⁴ (2) taken

enforcement

companies that made false

unsub

lending

investig

⁴ See, e.g.,

<https://www.ftc.gov/press-release/20150303-ftc-announces-resolution>

Resolution

<https://www.ftc.gov/press-release/20150303-ftc-announces-resolution>

⁵ See, e.g.,

<https://www.ftc.gov/press-release/20150303-ftc-announces-resolution>

Servs., Inc., N

<https://www.ftc.gov/press-release/20150303-ftc-announces-resolution>

Marketing LL

<https://www.ftc.gov/press-release/20150303-ftc-announces-resolution>

solutions-llc

123 (S.D. Fla. Mar. 4, 2015), available at <https://www.ftc.gov/press-release/20150303-ftc-announces-resolution>; *FTC v. Worldwide Info*

available at

<https://www.ftc.gov/press-release/20150303-ftc-announces-resolution>; *FTC v. All Us*

015), available at

<https://www.ftc.gov/press-release/20150303-ftc-announces-resolution>

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.

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

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.

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

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