KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org
CENTER FOR DEMOCRACY & TECHNOLOGY

Issue Brief: Weakening ECPA Reform By Altering Emergency Exception Rule Unnecessary and Problematic

July 10, 2015

Current Practices Regarding Emergency Exceptions

Generally electronic communications providers cannot give content and sensitive user information to the government absent a court order. However, the law does contain an exception so that in an emergency situations involving danger of death or serious bodily harm, the provider may disclosure content and user records to law enforcement absent a court order.[1] Because these requests receive no independent judicial oversight, providers have discretion to assess whether the request is proper and should be fulfilled absent a court order. As ECPA reform legislation continues to gather strong support, some have called for a new provision changing this rule to mandate compliance with any emergency request for user data or content. Such a change is both unnecessary, and would raise significant privacy and security problems.

Mandatory and Unchecked Disclosure Would Lead to Misuse

Requiring providers to comply with any and all emergency requests would lead to misuse and improper demands, as evidence by past activities.

Although most emergency requests are considered appropriate and complied with, there are enough instances where requests are deemed improper that providers' authority to evaluate their legitimacy should not be disregarded. For example, in 2014, Google rejected 94 out of 342 requests.

Government has previously abused its ability to engage in emergency requests. A 2010 Department of Justice Inspector General report stated that the Inspector General "found repeated misuses of [the FBI's] statutory authority to obtain telephone records through NSLs or the ECPA's emergency voluntary disclosure provisions."[2] Based on this, the Inspector General report recommended Congress consider "appropriate controls" on the FBI's ability to obtain records in emergency situations. With mandatory compliance and no judicial oversight, such abuses could become more frequent.

Service providers act as the only check to ensure the legitimacy of requests and prevent abuse, as the law intends. ECPA permits providers to give user information to the government if "the provider, *in good faith*, believes that an emergency involving danger of death or serious physical injury to any person … requires disclosure without delay."[3] Abandoning this system in favor of mandatory compulsion would remove all independent authority to evaluate the legitimacy of requests, eliminating providers as the only protection from misuse.

---

[1] See, 18 U.S.C. §§ 2702(b)(8) & (c)(4).
[2] *See*, Office of the Inspector General, Department of Justice, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (January 2010), 268, *available at* https://oig.justice.gov/special/s1001r.pdf.
[3] 18 U.S.C. § 2702(c)(4) (emphasis added).

Mandatory Approval of Government Requests Is Unnecessary

Requiring providers to comply with any emergency request for user data or content is also unnecessary. Emergency requests are rare. America's largest Internet and electronic communications companies only receive a small number of requests. For example, Google only received 342 emergency requests[4] and Microsoft only received 475 requests[5] throughout all of 2014. In comparison, Google received 20,280 subpoenas and search warrants and Microsoft received 12,364 similar requests during that same year.

And while the number of requests is very small, most government emergency requests for data and content are granted. In 2014, Google, Facebook,[6] Microsoft, and Yahoo![7] all provided data for the majority of emergency requests received.

In the event that a provider does not think a request is proper, the government still has available options. Law enforcement can revise its request to obtain content or data if appropriate justification has not been provided. Additionally, government entities may also seek information through ECPA's mandatory disclosure provisions without delay. In all judicial districts a magistrate is available for after-hours requests that require immediate action, and Rule 41 of the Federal Rules of Criminal Procedure stipulates for telephonic search warrants to be obtained at all hours.

Mandatory Disclosure Would Risk Data Security

Requiring providers to comply with any emergency requests would endanger data security by interfering with providers' ability to assess the validity of requests. Data thieves regularly attempt to take customer information by posing as law enforcement and demanding that data be provided pursuant to an emergency. Congress criminalized this activity because of the serious threat it posed.[8] Providers must have the capability to ensure that requests are not fraudulent, or made in a manner that unnecessarily risks disclosure of user data to unauthorized third parties. Mandating disclosure in response to all emergency requests and removing discretion to appeal for clarification, additional information, or a more secure method of disclosure would undercut providers' ability to protect users' sensitive information.

Conclusion

The current system for disclosure of user information and content pursuant to emergency requests absent a court order works effectively. It protects both public safety and user privacy and security, and should not be changed. Providers take seriously both safety needs and their users privacy rights. Voluntary disclosure that assesses government requests allows them to effectively protect both.

---

[4] *See*, *Google Transparency Report: Security and Privacy*, *available at* http://www.google.com/transparencyreport/userdatarequests/US/.
[5] *See*, *Microsoft Law Enforcement Requests Report*, *available at* https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.
[6] *See*, *Facebook Government Requests Report: United States Law Enforcement Request for Data*, *available at* https://govtrequests.facebook.com/country/United%20States/2014-H1/.
[7] *See*, *Yahoo! Transparency Report: Government Data Requests*, *available at* https://transparency.yahoo.com/government-data-requests/index.htm (Data on number of emergency requests and number granted was provided as a global aggregate).
[8] See, 18 U.S.C. 1039.