

Blog Round Up: Experts on CALEA II Proposal

by [Nasreen Hosein](#) [1]
May 17, 2013

[CALEA II: Risks of wiretap modifications to endpoints](#) [2]

[Edward W. Felten](#) [3] is a Professor of Computer Science and Public Affairs at Princeton University, and the founding Director of Princeton's Center for Information Technology Policy. Felten was the Federal Trade Commission's first Chief Technologist.

Our report argues that mandating a virtual wiretap port in endpoint systems is harmful. The port makes it easier for attackers to capture the very same data that law enforcement wants. Intruders want to capture everything that happens on a compromised computer. They will be happy to see a built-in tool for capturing and extracting large amounts of audio, video, and text traffic. Better yet (for the intruder), the capability will be stealthy by design, making it difficult for the user to tell that anything is amiss.

[The FBI's New Wiretapping Plan Is Great News for Criminals](#) [4]

[Bruce Schneier](#) [5] is an internationally renowned security technologist and author. He has testified on security before the United States Congress on several occasions and has written articles and op-eds for many major publications, including *The New York Times*, *The Guardian*, *Forbes*, *The San Francisco Chronicle*, and *The Washington Post*.

The FBI wants a new law that will make it easier to wiretap the Internet. Although its claim is that the new law will only maintain the status quo, it's really much worse than that. This law will result in less-secure Internet products and create a foreign industry in more-secure alternatives. It will impose costly burdens on affected companies. It will assist totalitarian governments in spying on their own citizens. And it won't do much to hinder actual criminals and terrorists.

[Center for Democracy and Technology Report on USG Proposals to Expand CALEA to Peer-to-Peer Communications](#) [6]

[Susan Landau](#) [7], Guggenheim Fellow, Author of *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*

Our first concern is something that I have written about on multiple occasions, namely that an architected security breach—which is what a wiretap is—is exploitable not only by law enforcement but also by criminals, other nation states, etc. Then, to satisfy law enforcement, companies must either enable a 24/7 capability for wiretapping whenever law enforcement requires it or — very dangerous — give any law-enforcement organization, no matter how small and poorly secured, the ability to conduct the tap on its own. This is really dangerous.

[“Going Dark” vs. “Going Secure” New CDT Experts’ Report on CALEA II](#) [8]

[Peter P. Swire](#) [9] is the C. William O’Neill professor of law at the Moritz College of Law of the Ohio State University. He is a senior fellow with the Future of Privacy Forum and the Center for American Progress and policy fellow with the Center for Democracy and Technology. Under President Clinton, he served as Chief Counselor for Privacy in the U.S. Office of Management and Budget.

Building holes and backdoors into widely-available software and services creates vulnerabilities that can be exploited by a range of bad actors, including hackers, individual employees at the software companies and government officials in the numerous countries that will expect the same access afforded to the FBI. When it comes to cybersecurity online, the first rule for government should be 'do no harm.'

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://www.cdt.org/blogs/nasreen-hosein/1705blog-round-experts-calea-ii-proposal>

Links:

- [1] <https://www.cdt.org/personnel/nasreen-hosein>
- [2] <https://freedom-to-tinker.com/blog/felten/calea-ii-risks-of-wiretap-modifications-to-endpoints/>
- [3] <http://www.cs.princeton.edu/~felten/>
- [4] http://www.foreignpolicy.com/articles/2013/05/29/the_fbi_s_new_wiretapping_plan_is_great_news_for_criminals
- [5] <http://www.schneier.com/about.html>
- [6] <http://www.lawfareblog.com/2013/05/center-for-democracy-and-technology-report-on-usg-propos-als-to-expand-calea-to-peer-to-peer-communications/>
- [7] <http://privacyink.org/>
- [8] https://www.privacyassociation.org/privacy_perspectives/post/going_dark_vs._going_secure_new_cdt_experts_report_on_calea_ii
- [9] <https://www.cdt.org/personnel/peter-swire>