Steven M. Bellovin
Columbia University

The Law and Lawful Hacking

I'm on record[1] as being in favor of "lawful hacking"—law enforcement hacking into computers—as preferable to putting back doors into encryption systems. There's just one problem: in the United States, at least, there's not a specific statute that actually permits this. And that matters, because were there an explicit statute, there would be public debate, not just on the concept itself—and it is controversial—but to establish the necessary limits and restrictions. (I'll speak of American law, because it's the legal system I know best, but the underlying issues are fundamental and apply to democracies worldwide.)

To start (and as I've written elsewhere[2]), what are known as *remote computer searches* are potentially dangerous. Even vendor patches have been known to "brick" systems, and vendor update systems have the advantage that the target computer can "pull" the proper patches for its configuration. Code inserted by police generally can't do that, and thus poses a greater risk. This is not to say that such searches should not be done, but the risk to innocent parties—and such searches are not done only on guilty or even presumed-guilty parties' computers—should be weighed against the anticipated benefits of the search.

There are also privacy issues to consider. Computers can hold a vast amount of personal information, and are often shared with family members. A few years ago, the U.S. Supreme Court noted that cell phones can hold "all the privacies of life"—but phones are targets of lawful hacking, too. All searches are intrusive, but remote hacking is more so, partially because you don't know if you're getting the right computer or who else might have information stored on it.

The United States has been through a similar debate before over another invasive technology: wiretapping. Especially in the days before cell phones, a tap on a phone line exposed the conversations of anyone else who used that line, especially family members. One Supreme Court justice called wiretapping a "dirty business"; another called it an instrument of "tyranny and oppression." A former chair of the Federal Communications Commission called wiretappers "the least admirable of the groups of creatures that qualify for membership in the human race… [who] would be frightened by the noonday sun." The answer, though, was not to give up wiretapping, but to restrict it, an answer that was proposed at least as early as 1952, 16 years before the country passed a statute authorizing it. Thus, wiretaps can only be used when investigating a certain specified list of offenses, and only if other investigative techniques have failed or would be unreasonably dangerous.

We need some restrictions on lawful hacking. Perhaps it could be used for, say, investigation of terrorism but not for copyright infringement. Perhaps the warrant application should specify why police believe that the particular computer to be hacked is *the* right one and not one belonging to another family member. Or perhaps that isn't a reasonable restriction, if going through a family member's computer is the best way to get at the targets.

That, though, is precisely the point: the issue has never been debated. An explicit statute would be a good idea in its own right, but the public debate—the committee hearings, the witnesses, the amendments, the tradeoffs—would be more valuable still. If we're going to have lawful hacking, we need to have a *law*. ■

Digital Object Identifier 10.1109/MSEC.2021.3077374
Date of current version: 1 July 2021

References

1. S. M. Bellovin, M. Blaze, S. Clark, and S. Landau, "Going bright: Wiretapping without weakening communications infrastructure," *IEEE Security Privacy*, vol. 11, no. 1, pp. 62–72, Jan.–Feb. 2013. doi: 10.1109/MSP.2012.138.
2. S. Bellovin, M. Blaze, and S. Landau, "Insecure surveillance: Technical issues with remote computer searches," *Computer*, vol. 49, no. 3, pp. 14–24, 2016. doi: 10.1109/MC.2016.68.

Steven M. Bellovin is a professor of computer science and affiliate law faculty at Columbia University. Contact him via https://www.cs.columbia.edu/~smb.