



Why is this greyhound smiling?  
Click here to find out!

Protecting  
Greyhounds  
Nationwide  
GREY2K USA

## Government Snooping in a Digital Age

**A newly updated book on telecom surveillance shows how the president's expanded intelligence-gathering powers go way beyond tapping phone lines -- and why we should all be very, very concerned.**

AZIZ HUQ | August 23, 2007 | web only

[Privacy on the Line: The Politics of Wiretapping and Encryption](#) by Whitfield Diffie and Susan Landau (*The MIT Press*, 400 pages)

---

Less than ten years ago, two respected research engineers wrote a book about privacy and telecommunications. In large measure, that book, by Whitfield Diffie and Susan Landau, focused on cryptography -- the science of encrypting information -- and the Clinton administration's insistence on installing "escrow" devices, or backdoors into encryption systems, that only it could access.

Today, that debate on encryption seems rather quaint. The Patriot Act now endorses government "carnivore" programs that can gather information about who visits what Web sites. Since 2001, the National Security Agency has been conducting a massive program of warrantless electronic surveillance of both domestic and foreign communications with the cooperation of all but one U.S. telecommunications carrier. And just this month, the Protect America Act punched a Mack truck through privacy protections for Americans' electronic communications, abolishing core judicial and congressional restraints on NSA surveillance by amending the 1978 Foreign Intelligence Surveillance Act (FISA).

So Diffie and Landau picked a perfect time to release their newly updated and expanded edition of that book, *Privacy on the Line*, a primer for non-specialists on the nitty-gritty of telecommunications and surveillance. (Their first edition, to be fair, fell into obsolescence years ago given its focus on cryptography: The copy I retrieved from New York University's library had not seen daylight for a while.)

There are difficult questions to be answered about how privacy works, and the value it holds in our increasingly data-driven world. Diffie and Landau do not provide comprehensive answers, but their airing of the technical questions is helpful in understanding the pressing issues raised by the Protect America Act and its ilk.

Three large trends in telecommunications discussed by Diffie and Landau converge to create these pressing issues.

First, today's new media of communication do not merely replace existing alternatives, but supplement them in ways that become unavoidable. Twenty years ago, email and internet teleconferences were inconceivable. Today, they are not only possible, but they are the sole and sometimes unavoidable means to communicate to someone on the other side of the globe. These new electronic media are simply facts of everyday life today. .

Second, there have been geometric increases in the volume of data each individual creates each day: Every time your paycheck comes through; every time you swipe your credit card; every time you pick up the phone or log on to the *Prospect* site, a record is created. A trail of electronic flotsam is left behind. And as computing power increases, it becomes easier and easier for the state to reconstruct that trail and thereby to map an individual's voyage through the world.

Finally, new media have radically shifted the balance of power between the individual and the government. Once, you and I could be assured of privacy by stepping out into a secluded lane or wood. Now, parabolic listening devices, effective at a distance, make that unreliable. And since neither you nor I have the wherewithal to construct an electronic router -- one of the massive hubs used to channel and direct packets of telephone or email signal -- our alternatives are limited. Technology has tipped the scales in the government's favor.

Further, as Diffie and Landau caution, the telecommunications field is in fact dominated by a small coterie of corporate actors who have created only a limited number of facilities. Practically speaking, you and I have little choice as to which wires carry our telephone calls and emails.

Moreover, the absence of privacy is often grafted into the very architecture of electronic communication. One of the most interesting parts of Diffie and Landau's book concerns the 1994 Communications Assistance for Law Enforcement Act, or CALEA, which "puts the government right in the middle of the process of designing telephone switches." Indeed, it's partially thanks to this (Clinton-era) law that the NSA could move so smoothly into massive warrantless surveillance.

As Diffie and Landau's account makes clear, these trends, with other developments, have wholly shifted both the nature of privacy and the nature of the threat to privacy. What right to privacy do we have, or should we have, in our amassed financial history? In our telephone records? Our internet habits? What if we accrue these records with barely a thought to who can listen in? And does the mere fact that government has access to this data -- either directly or indirectly through its purchase in the marketplace -- ring alarm bells? Or is the real question precisely what the state will do with the information in its possession?

The problem today is that the public lacks not only the technical details necessary to understand these questions, but it also has no evaluative framework to wrestle with them. We are too often inconsistent with our own privacies: Recklessly free with our use of credit cards when we purchase a book, yet outraged when our library usage is tracked. Nor have we grappled with the hard questions by statutes like CALEA, which build government in to the very architecture of communication -- effectively giving the state a monopoly on *our* privacy.

This month's Protect America Act is a good example of how the federal government can seize opportunities created by our failure to think hard about these questions -- and use its advantage to tip the playing field further in its favor.

Section 105A of that law exempts from any meaningful judicial or congressional surveillance any spying that the government "reasonably believes" to be "directed" at a foreign person. Under this provision, the NSA could scoop up all the calls made from a U.S. phone on the logic that most of its calls were made to foreign numbers, and hence the spying was "reasonably believed" to be focused overseas.

The less-noticed section 105B, meanwhile, is nebulously crafted in a way that seems to repeal checks imposed by the Communications Act and the Stored Communications Act on the gathering of non-content information (such as the telephone numbers you call or that call you), and also to expand the government's authority to force telecom carriers to enable real-time acquisitions of large streams of data.

None of these new powers was debated in Congress in any meaningful way. Nor is it clear how security is enhanced by many of them. For example, the section 105A exception for domestic-to-foreign surveillance is, for the first time, not tethered to a security justification. It seems to permit warrantless interception of U.S.-to-overseas calls for all reason or no reason at all. And since section 105B is unclear in scope, its precise impact on privacy remains to be seen.

Diffie and Landau provide useful thumbnail sketches of many of the technical issues at play in this debate. Only in the last few pages of their book, however, do they attempt to put the pieces together. But their synthesis is meager. Rather, *Privacy on the Line* is best used as a background resource, dipped into for specific information about technical questions.

Even then, the book is not without flaws. The history of intelligence abuses in the Cold War era is unhelpfully repeated in multiple chapters. There is insufficient discussion of how external enemies might penetrate or assail American telecommunications networks -- and as the attack on Estonian networks in late April this year made clear, electronic warfare is hardly unlikely. There are also some factual errors that, while irrelevant in themselves, prick at the reader's confidence. (For example, the law creating the CIA was called the National Security Act, not the Central Intelligence Act.)

With luck, the paperback edition will correct these minor flaws. Diffie and Landau deserve a large audience. Their lucid exposition adds valuable context to debates that for too long have been abstract, even if they do not answer the difficult evaluative questions raised by the evolving meaning of privacy in a digital world.

★★



**Aziz Huq** directs the Liberty & National Security Program at the Brennan Center for Justice at NYU, and is an associate professor of law at NYU. His book, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (with Fritz Schwarz) will be out in paperback in 2008.

