THE Nation.

Surveillance Can't Make Us Secure

by **JULIAN SANCHEZ**

January 29, 2010

In a major **speech** on Internet freedom last week, Secretary of State Hillary Clinton urged American tech companies to "take a proactive role in challenging foreign governments' demands for censorship and surveillance." Her call to action followed a series of dazzlingly sophisticated **cyberattacks** against online giant Google and more than thirty other major technology companies, believed to originate in the People's Republic of China. Few observers have found the Chinese government's staunch **denials** of involvement persuasive--but the attacks should also spur our own government to review the ways our burgeoning surveillance state has made us more vulnerable.

The Google hackers appear to have been interested in, among other things, gathering information about Chinese dissidents and human rights activists--and they evidently succeeded in obtaining account information and e-mail subject lines for a number of Gmail users. While Google is understandably reluctant to go into detail about the mechanics of the breach, a source at the company told **ComputerWorld** "they apparently were able to access a system used to help Google comply with [US] search warrants by providing data on Google users." In other words, a portal set up to help the American government catch criminals may have proved just as handy at helping the Chinese government find dissidents.

In a way, the hackers' strategy makes perfect sense. Communications networks are generally designed to restrict outside access to their users' private information. But the goal of government surveillance is to create a breach-by-design, a deliberate backdoor into otherwise carefully secured systems. The appeal to an intruder is obvious: Why waste time with retail hacking of many individual targets when you can break into the network itself and spy wholesale?

The Google hackers are scarcely the first to exploit such security holes. In the summer of 2004, unknown intruders managed to activate **wiretapping software** embedded in the systems of Greece's largest cellular carrier. For ten months, the hackers eavesdropped on the cellphone calls of more than 100 prominent citizens--including the prime minister, opposition members of parliament, and high cabinet officials.

It's hard to know just how many other such instances there are, because Google's decision to go public is quite unusual: companies typically have no incentive to spook customers (or invite hackers) by announcing a security breach. But the little we know about the existing surveillance infrastructure does not inspire great confidence.

Consider the FBI's Digital Collection System Network, or **DCSNet**. Via a set of dedicated, encrypted lines plugged directly into the nation's telecom hubs, DCSNet is designed to allow authorized law enforcement agents to initiate a wiretap or gather information with point-and-click simplicity. Yet a 2003 internal audit, released several years later under a freedom-of-information request, found a slew of problems in the system's setup that appalled security experts. Designed with external threats in mind, it had few

safeguards against an attack assisted by a Robert Hanssen-style accomplice on the inside. We can hope those problems have been resolved by now. But if new vulnerabilities are routinely discovered in programs used by millions, there's little reason to hope that bespoke spying software can be rendered airtight.

Of even greater concern, though, are the ways the government has encouraged myriad private telecoms and Internet providers to design for breach.

The most obvious means by which this is happening is direct legal pressure. State-sanctioned eavesdroppers have always been able to demand access to existing telecommunications infrastructure. But the Communications Assistance for Law Enforcement Act of 1994 went further, requiring telephone providers to begin building networks ready-made for easy and automatic wiretapping. Federal regulators recently expanded that requirement to cover broadband and many voice-over-Internet providers. The proposed SAFETY Act of 2009 would compound the security risk by requiring Internet providers to retain users' traffic logs for at least two years, just in case law enforcement should need to browse through them.

A less obvious, but perhaps more serious factor is the sheer volume of surveillance the government now engages in. If government data caches contain vast quantities of information unrelated to narrow criminal investigations--routinely gathered in the early phases of an investigation to identify likely targets--attackers will have much greater incentive to expend time and resources on compromising them. The FBI's database now contains billions of records from a plethora of public and private sources, much of it gathered in the course of broad, preliminary efforts to determine who merits further investigation. The sweeping, programmatic NSA surveillance authorized by the FISA Amendments Act of 2008 has reportedly captured e-mails from the likes of former President Bill Clinton.

The volume of requests from both federal and state law enforcement has also put pressure on telecoms to automate their processes for complying with government information requests. In a **leaked recording** from the secretive ISS World surveillance conference held back in October, Sprint/Nextel's head of surveillance described how the company's L-Site portal was making it possible to deal with the ballooning demand for information:

> "My major concern is the volume of requests. We have a lot of things that are automated, but that's just scratching the surface.... Like with our GPS tool. We turned it on--the web interface for law enforcement--about one year ago last month, and we just passed 8 million requests. So there is no way on earth my team could have handled 8 million requests from law enforcement, just for GPS alone. So the [L-Site portal] has just really caught on fire with law enforcement. They also love that it is extremely inexpensive to operate and easy, so, just the sheer volume of requests.... They anticipate us automating other features, and I just don't know how we'll handle the millions and millions of requests that are going to come in."

Behold the vicious cycle. Weakened statutory standards have made it easier and more attractive for intelligence and law enforcement agencies to seek information from providers. On top of the thousands of wiretap and so-called "pen/trap" orders approved each year, there are *tens* of thousands of National Security Letters and subpoenas. At the ISS World conference, a representative of Cricket, one of the smaller wireless providers, estimated that her company gets 200 law enforcement requests per day, all told; giants like **Verizon** have said they receive "tens of thousands" annually. (Those represent distinct legal demands for information; Sprint's "8 million" refers to individual electronic requests for updates on a target's location.)

Telecoms respond to the crush of requests by building a faster, more seamless, more user-friendly process for dealing with those requests--further increasing the appeal of such tools to law enforcement. Unfortunately, insecurity loves company: more information flowing to more legitimate users is that much more difficult to lock down effectively. Later in his conference, the Sprint representative at ISS World speculated that someone who mocked up a phony legal request and faxed it to a random telecom would have a good chance of getting it answered. The recipients just can't thoroughly vet every request they get.

We've gotten so used to the "privacy/security tradeoff" that it's worth reminding ourselves, every now and again, that surrendering privacy does not automatically make us more secure--that systems of surveillance can themselves be a major source of *in*security. Hillary Clinton is absolutely right that tech companies seeking to protect Internet freedom should begin "challenging foreign governments' demands for censorship and surveillance." But her entreaty contains precisely one word too many.

About Julian Sanchez

Julian Sanchez is a research fellow at the Cato Institute and a contributing editor for *Reason* magazine. You can read his personal blog **here**. **more...**