

*Cato scholars on the NSA's transgressions*

## Unveiling the Surveillance State

In early June of this year, journalist Glenn Greenwald began a series of articles for the *Guardian* disclosing the operational details of numerous mass surveillance programs conducted by the U.S. National Security Agency (NSA). The subsequent scandal that erupted revealed a large-scale overcollection of the phone and Internet communications of all Americans by government agencies.

In Greenwald's early stories breaking the scandal, Cato's Julian Sanchez was featured prominently to discuss the nature of these revelations. A research fellow at the Institute, Sanchez emphasized in particular what makes email metadata different from other forms of private information. "The calls you make can reveal a lot," he told Greenwald, "but now that so much of our lives are mediated by the internet, your IP logs are really a real-time map of your brain: what are you reading about, what are you curious about, what personal ad are you responding to (with a dedicated email linked to that specific ad), what online discussions are you participating in, and how often?"

This information, in other words, can be incredibly revealing. "Seeing your IP logs—and especially feeding them through sophisticated analytic tools—is a way of getting inside your head that's in many ways on par with reading your diary," he continued.

Sanchez has emerged as one of the leading voices at the busy intersection between technology, privacy, and civil liberties. In August, *Wired* listed him as one of the top 15 government and security resources to follow—"reporters and researchers [who] can be counted on to give you the news that matters about the state of law and security." Sanchez was identified specifically for his "timely yet profoundly moral commentary on privacy and surveillance issues."

He was also a regular resource for the *Washington Post* on surveillance stories, telling one reporter that Chief Justice John Roberts is "single-handedly choosing the people who get to decide how much surveil-



At an expert briefing in June hosted by the Congressional Internet Caucus Advisory Committee, **JULIAN SANCHEZ**, research fellow at the Cato Institute, outlined the NSA's spying scandals to Capitol Hill staffers. He spoke in particular about the "dangerous shift" in the way the Fourth Amendment has been interpreted.

lance we're subject to."

The ability to indiscriminately vacuum up the communications of Americans under sweeping authorities amounts to clear civil liberties' violations. "When the NSA scandal erupted, we saw something that hasn't been seen on the American continent in more than 200 years: a general warrant," wrote Jim Harper, Cato's director of information policy studies. According to the Constitution, a warrant must meet two criteria. First, it must be based on probable cause. Second, it must describe *in particular* the place to be searched and the person or things to be seized. The warrants in this case satisfied neither.

"The Fourth Amendment flatly bars general warrants, but the NSA has cajoled the Foreign Intelligence Surveillance Court into giving it access to data about every American's communications, without regard to suspicion," Harper added. The plan, it seems, was to collect both phone and internet data—storing it indefinitely—so that when suspicion arose about somebody in the future, the agency could investigate that person. This essentially amounts to what Harper calls "a future-crime unit."

As technology grants intelligence agencies a dizzying array of new ways to spy—on

a scale that would have sounded like science fiction a decade ago—the potential for privacy abuse is clear. But, in many ways, mass surveillance threatens a much more fundamental right as well.

In one of her recent *Wall Street Journal* columns, Peggy Noonan profiled Nat Hentoff, asking the renowned journalist about his thoughts on the implications of domestic surveillance. Hentoff, a senior fellow at the Cato Institute and one of the leading First Amendment advocates of the past half-century, agreed that the Fourth Amendment is at stake. "Broad and intrusive surveillance will, definitively, put government in charge," Noonan wrote. "But a republic only works, Mr. Hentoff notes, if public officials know that they—and the government itself—answer to the citizens."

Hentoff also noted, however, that the surveillance state can cause Americans to be more cautious of what they say. "If you don't have free speech you have to be afraid, you lack a vital part of what it is to be a human being who is free to be who you want to be," Hentoff told the *Journal*. The result is that freedom of expression suffers.

"The inevitable end of surveillance," Noonan drew from this, "is self-censorship." ■