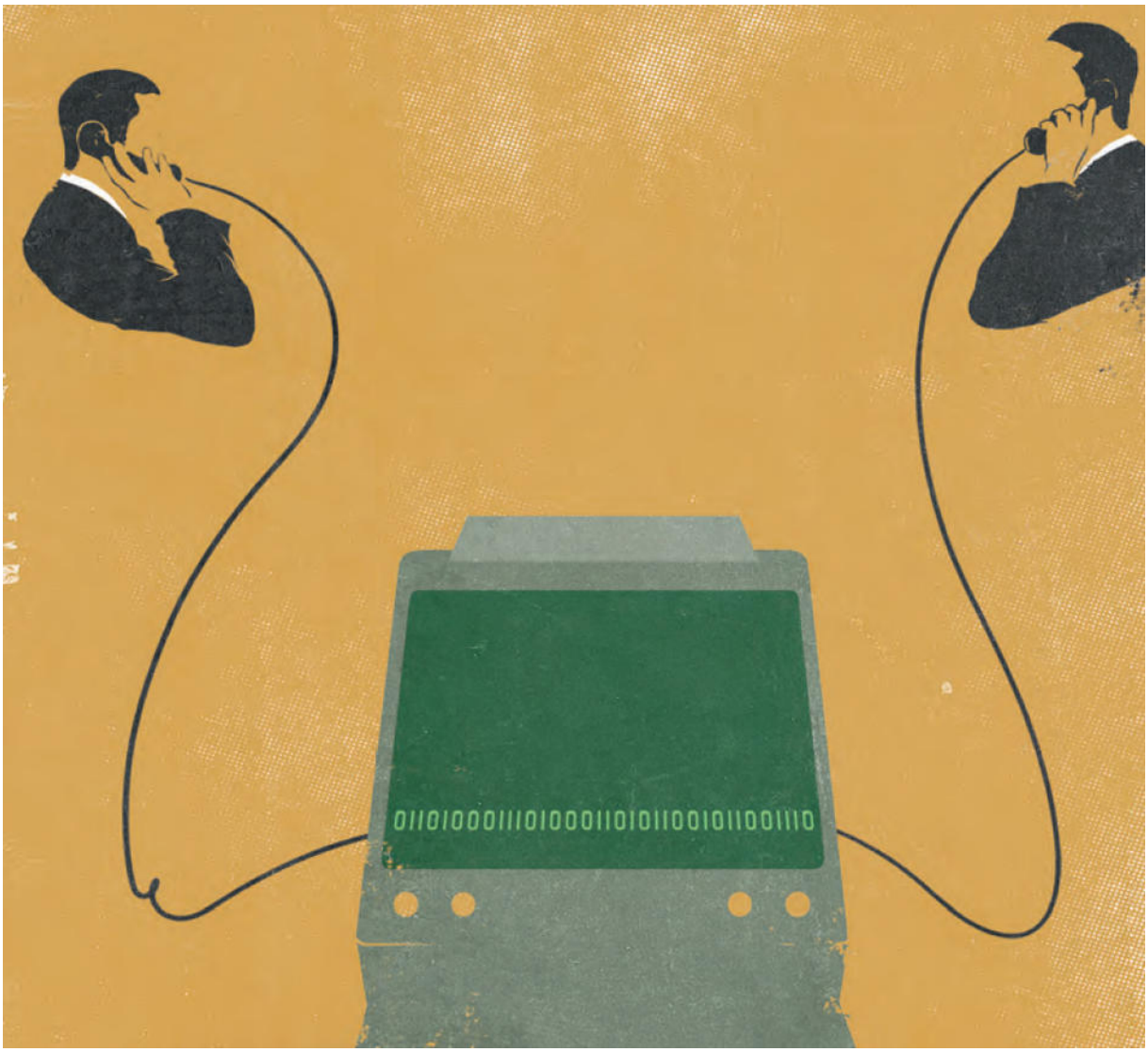
Science & Technology

A Secret History

By
Phoebe Magee
|
Winter 2014-15



Carlo Giambarresi

"They are getting everyone’s calls,” Edward Snowden told a *Guardian* reporter in his Hong Kong hotel room in May 2013. “Everyone’s call records and everyone’s

Internet traffic as well."

"They," of course, is the United States National Security Agency. And regardless of whether Snowden is a great traitor or great patriot, when he escaped the US with tens of thousands of the NSA's classified documents, the agency's activities were suddenly exposed. Snowden claims that at a certain point, he just couldn't abide the ever-increasing magnitude of the data collection and storage systems he helped create. The whistle was blown; we are being recorded.

Matthew Jones is the James R. Barker Professor of Contemporary Civilization at Columbia. As a historian of science and technology, Jones is working on a "historical and ethnographic account of big data" titled *Data Mining: The Critique of Artificial Reason*. He believes that the NSA revelations of 2013 demand closer inspection in light of their historical context: the decades in which computer use became normal and the amount of information gathered *about* computer users grew exponentially.

In November, Jones, with Harvard historian David Armitage, gave a talk at the Heyman Center for the Humanities called "Great Exploitations: History and the NSA Debate." The room was filled with humanities students raised in the Internet era and older people who wondered what companies were complicit in gathering their conversations. The history Jones wished to present, he said, was neither a "personality-driven" account (*Dick Cheney did it!*) nor a "classic libertarian tale of government expansion." Instead, Jones would outline a series of recent "transformations," moments between the mid-1990s and today when US government surveillance significantly changed.

The first transformation concerned the volume of data. In the mid-'90s, Jones said, dealing with the volume of information the NSA had collected "was [its] foremost problem internally." To address this, the agency created more and better computer programs to analyze all that it was gathering. This abundance of data allowed the NSA to devise a novel scheme called "contact chaining," said Jones. "Contact chaining is the idea that I take what's called a seed, a single person's telephone, and I connect all of the other telephones that telephone has called. Then I connect to the next step and maybe even another." The idea was to link domestic numbers to foreign numbers and thwart a possible terrorist attack. But to track information about phone calls made by US citizens without a warrant was, the Clinton DOJ decided, a violation of the Fourth Amendment.

Then, in 2007, a secret Justice Department memo under the Bush administration heralded a second transformation, shining a spotlight on “metadata” — information about information. Gatherers of metadata may not know what you said, but they know whom you said it to. The memo stated that henceforth, “contact chaining and other forms of metadata do not qualify as the ‘interception or selection of communication,’” and are therefore not illegal. President Barack Obama’s new administration upheld this.

Jones’s third transformation occurred between 1997 and 2013, as the United States government developed, in the words of Obama, “mature capabilities” to hack computers for data collection. This, Jones said with some gravity, “is internally referred to as ‘owning the net.’”

“The argument is made that it’s necessary to modernize surveillance law to keep up with technological developments,” he said. Writing in a new legal category for metadata, for example, is billed as a necessary “update” to existing law, but according to Jones, “that is far from obviously so.” A 1979 Supreme Court decision called *Smith v. Maryland* established that users of telephones have no reasonable expectation of privacy when it comes to the numbers that they dial, even if they expect privacy when it comes to the content of their calls. You don’t need a warrant to legally snoop on phone numbers a person dials — you only need one to *listen* to phone calls. This decision, Jones pointed out, was made when Americans were calling one another through copper wires. After 9/11, however, the division between dialing information and the content of the phone call became the division between metadata and the content of a phone call, a website, or an e-mail.

Jones called the Patriot Act of 2001 “mostly small emendations of definitions in the law.” *Smith v. Maryland* was about one guy with a landline. The Patriot Act expands the definition of dialing information — which, as decided in 1979, can be legally recorded and tracked — to include a much broader range of wire and electronic communication, such as e-mail. Among Jones’s sources is an FBI fact sheet responding to protests from the ACLU. The fact sheet says that “updating” dialing information to metadata in the law is simply keeping up with current technology. Furthermore, it allows law enforcement to defend the homeland by “collecting non-content information from terrorist organizations, regardless of what medium they use to communicate.” But Jones said it actually “takes a law about a landline and changes it to apply to many more technologies.” *Smith v. Maryland* was about “one guy,” said Jones, but here, it was being used as grounds for “wiretapping not you, or

me, but everyone.”

As he put it, “no one cares about metadata for one guy.” But if you collect a ton of information about everybody, contrasts within that information take on importance. You can learn a lot, he said, by studying “external communication without content,” similar to looking at the address on the envelope without reading the letter. If you see envelopes, for example, “from a family doctor and then an oncologist, you can find out that someone is seriously ill without reading more than an address.” Learning from patterns of communication, without necessarily reading any messages, is called traffic analysis, and it’s something the NSA has done “for decades,” said Jones. “It’s central to their internal identity.” What’s changed is the target: not military communications, but all communications.

Jones told his audience that he hoped to illuminate “two domains of profound arcana: arcane aspects of telecommunications, and really arcane aspects of national security.” He said they are “incredibly boring,” but shying from them preserves the idea that “people don’t understand and shouldn’t get involved.”

In pondering the transformations we are living through, we might question whether changes in the law truly make our society better. The job of the intelligence community, and particularly the NSA, is to “exploit” communications: to make use of them. Jones argues that the law, and people’s fears, should not be exploited in the process.

Read more from
Phoebe Magee

Guide to school abbreviations

All categories >
Read more from
Phoebe Magee