Being watched: Surveillance and the Christian community

by Daniel Schultz in the July 10, 2013 issue

© Ryan McVay

In recent weeks, revelations about government surveillance have highlighted the size and scope of U.S. intelligence operations in the post-9/11 world. Initial reports from the *Washington Post* and the *Guardian* suggested that federal agencies—primarily the National Security Agency—have been using secret programs to collect information on all calls and text messages placed to or from the U.S. through Verizon phone networks (and presumably others). Likewise, the NSA appears to be accumulating information on e-mails, chat sessions and other online communication—with assistance from companies such as Microsoft, Google, Yahoo and Apple.

These tech companies assert that the NSA does not have direct access to their data. Instead, they maintain that they have installed special “lockbox” servers onto which they can load specific information requested through a court order—a far smaller slice of the entire pie. Intelligence agencies can then download the material, along with instructions on how to parse what remain very large data sets. Without this assistance from the companies, the government argues, interpreting the information would take far too long to be useful.

Big tech is eager to reassure customers that the government has only limited access to personal information. Facebook, for example, has released data showing that fewer than 19,000 accounts (out of 1.1 billion total) were accessed by government agencies at any level in the second half of 2012. Closer scrutiny of leaked NSA documents seems to back up the companies' claims that government spies are able to look only at materials provided to them on the lockbox servers. At the moment, the government doesn't appear to be able to conduct blanket surveillance of electronic communications.

But reports by whistleblowers allege that the government has built special switches into the physical structure of telephone networks that allow them to drink directly from the data firehose. And public information about the workings of the NSA suggests that it is building data farms capable of intercepting, storing and deciphering all phone and online traffic in the U.S.—an enormous undertaking, and one shrouded in secrecy. The NSA appears to see its mission as part of a greater cyberwar capability that includes infrastructure defense, hacking and "cyber-kinetic" attacks such as Stuxnet, the computer worm used to disrupt the Iranian nuclear program.

Still, the NSA and other agencies are rarely interested in the actual content of phone calls or e-mails, all late-night jokes and editorial cartoons aside. Access to such specifics requires a warrant attesting to probable cause.

What government agents can access more easily is metadata: information about, say, the numbers dialed from a cell phone, when and from where. This can reveal a lot, all without listening in on a single call. A reporter's call records can pinpoint their sources for leaks. Much can be ascertained about someone's health based on the specific medical specialists he or she dials. And extramarital affairs can be exposed simply by showing where a cell phone spent the night. Online metadata can be just as revealing. In one study, researchers at MIT were able to out gay men using nothing but their friend lists on Facebook.

The ability to analyze a person's social connections has been around for a while. Not surprisingly, it's gotten more sophisticated with the rise of social media and big data. Law enforcement agencies have used such data to catch fugitives and track terrorist cells. It's how they caught Khalid Sheikh Mohammed, among others.

In repressive nations, the same techniques have been used to monitor and disrupt opposition groups. It's remarkably easy to use connections made through cell phones and social media to convince people that they're being watched 24/7. This makes dividing and conquering a snap: all it takes is a visit from the police or, even better, an anonymous e-mail or call.

That's the thumbnail version of what we know about electronic intelligence gathering these days. What we don't know may be of greater concern. The Foreign Intelligence Surveillance Act of 1978 mandated a special court to oversee government intelligence collection in the U.S. But the FISA court is closed to the public: only the government is allowed to present evidence, and the details of how the court interprets the relevant laws are kept secret.

We don't know exactly what information the NSA collects, how, how much or at what expense. Given the recent penchant for outsourcing government work, we're not even sure whether it's federal employees or civilian contractors doing the spying. Nor do we know how effective the surveillance programs are, the extent of congressional supervision, or any misuses of the power that might have occurred. We don't even know how long these programs have been in place—or the legal justifications used in deciding whom to target.

Given the uncertainty and the fast-developing story, it's little wonder that there has been minimal reaction by religious groups. A quick survey of eight denominations found that only one—the Presbyterian Church (U.S.A.)—had a statement on government surveillance, dating from 2006. Another PCUSA statement from 2012 spoke of the church's support for civil liberties. The Southern Baptist Convention recently passed a resolution upholding "the freedom of the individual to live in accordance with his or her religiously informed values and beliefs," without specifically mentioning surveillance. Two other denominations indicated that statements might be forthcoming, as their leaders had time to consider the situation. Likewise, there has been only a smattering of talk from religious activists, individually or collectively. *[UPDATE: See the correction below.]*

How *should* faithful people react? We need a more developed theological ethics of what it means to live in an age when so much information about ourselves is so readily available—to friends, strangers, commercial interests and government agents alike. Likewise, more theological work needs to be done on the ethics of surveillance. Some scholars, such as Eric Stoddart, Kevin Macnish and Daniel Bell Jr.,

have begun work in the area. But it could be years before these concerns are fully explored.

In the meantime, David Omand, former head of Britain's counterpart to the NSA, offers a start in a recent *Guardian* op-ed. Echoing the just war tradition, Omand suggests several criteria for the use of data collection: sufficient sustainable cause (i.e., no fishing expeditions), integrity of motive, proportionate methods, right and lawful authority, reasonable prospect of success, secret intelligence collection only as a last resort.

Of course, these criteria are for people in power, the ones running the spy programs. What about the rest of us? We can be citizens, first of all, demanding more public accountability. It is absurd—and contrary to American values—for us not to know what kind of data is being collected on U.S. citizens, how it's acquired and for what purposes. The FISA court should be less secretive, and less of the congressional oversight of the intelligence apparatus should be done behind closed doors.

More oversight is needed as well. Both U.S. Director of National Intelligence James Clapper and Attorney General Eric Holder have been caught in demonstrable lies about surveillance programs, but they've faced no demonstrable consequences. Meanwhile, senators and representatives have been curiously reluctant to challenge the Obama administration's claims—or to show the public what is being done in its name.

All this has real and tangible implications for religious people. As recently as 2006, the FBI was surveilling groups such as the American Friends Service Committee. It continues to infiltrate and otherwise monitor Muslim organizations, along with antitax activists, environmentalists and others. Membership in social and religious groups is an easy way to establish social networks ripe for analysis through metadata and other tools. Americans will have to decide—at the ballot box, if necessary—whether safety or religious privacy is more important.

Surveillance comes about as part of the government's promise to keep us safe and secure. That promise should be subject to relentless scrutiny. History shows how easily national security becomes conflated with maintaining the political status quo. Jesus, after all, was executed as a threat to the Roman government of Palestine.

Besides, Christians, Jews and Muslims alike affirm that only God can provide ultimate security—not invulnerability to threat but God's transformative support and

presence amid our vulnerability. That's a useful standard to apply when thinking about the value of intrusive programs like PRISM—which didn't pick up the threat posed by the Boston marathon bombers and which seems to have provided only incidental support in a couple of other cases. If these surveillance systems can't protect Americans from threats as unsophisticated as the Tsarnaev brothers, perhaps they are no better than the "bear patrols" portrayed on *The Simpsons*: expensive, showy demonstrations of resolve that do little to save anyone from what are incredibly rare events.

In other words: security theater is an idol. And it ought to be exposed in whatever form it takes, from electronic snooping to pat-downs at the airport.

Perhaps the first thing to be done in response to these revelations, however, is to consider what kind of people we are—and what kind of people we want to be. John Howard Yoder, writing about how the New Testament church taught itself, discusses another kind of surveillance:

> The gifts of prophet, teacher, moderator, etc., all contribute to the process of theological articulation. They contribute best if each has maximum liberty to contribute in its own way and if the exercise of those liberties is itself coordinated in the right way. . . . The one thing which the New Testament language on these matters gives us no ground for is the notion that the theological task could be exercised in isolation from the bearers of other gifts or *from the surveillance of the total community*. [emphasis added]

The work of knowing God and building one another up gives very good reason for watching and being watched. It is meant for the good of all, and it can be shared and received in public. But the spiritual gifts received by the first Christians, according to Yoder, come about through the use of "maximum liberty . . . coordinated in the right way." We do ourselves a disservice when we give in to the temptation to make ourselves as safe as possible at the expense of freedom.

We also fall off the way when we concede that surveillance is the province of a government seeking to identify the bad people and isolate them before they can do harm. The people of God know that that real safety and real freedom work the other way around: starting with the tiniest, most particular information about people and building from it a responsive and responsible community. It's a community that exists not to prevent bad but to do good.

CORRECTION: This article incorrectly suggests that the Presbyterian Church (U. S. A.) is the only major denomination to issue a statement on government surveillance. In fact the United Methodist Church adopted such a statement in 2008. We regret the error. —Ed.