the weekly Standard

Libertarians of La Mancha

Objections to NSA surveillance are too often fanciful.

By: Richard A. Epstein and Mario Loyola- July 8, 2013

The political tables have turned almost 180 degrees. President Obama uneasily defends surveillance programs of the National Security Agency, while his liberal and libertarian opponents accuse him of lawlessly abusing his powers. The spectacle might even be entertaining, were it not for its worrisome implications. Republicans, the most reliable constituency for the surveillance policies that have protected the nation since September 11, are starting to walk away from them.

Senator Rand Paul recently crowed that Edward Snowden, the NSA leaker now on the lam, will go down as "an advocate of privacy." His father, former GOP congressman Ron Paul, declared that "we should be thankful" for the "great service" Snowden did in "exposing the truth about what our government is doing in secret." Rank-and-file Republicans in the House have filed a bill to further stifle NSA surveillance, and Tea Party favorite Mike Lee is leading a similar effort in the Senate. At the libertarian Cato Institute (where Epstein is an adjunct scholar), privacy champions have assailed the "authoritarian measures that are advanced by the military, intelligence, and law enforcement agencies." These voices could inadvertently weaken support for national security programs to a dangerous degree.

What a difference five years makes. When, in 2008, a Democratic Congress voted to enshrine President George W. Bush's Terrorist Surveillance Program in the FISA Reform Act of 2008, virtually all opposition came from the left. Senator Jay Rockefeller, the bill's principal drafter, bent over backwards to accommodate the objections of liberal Democrats such as Russ Feingold, Chris Dodd, and Ron Wyden. Yet with every revision, liberal senators pressed ever-more unreasonable objections, until it became obvious to Rockefeller that no matter how many civil liberties safeguards the law contained, die-hard liberals would oppose it.

What emerged from these compromises was a bill that, if anything, has unduly restricted the ability of the government to detect potential terror plots. The bill severely limited the government's authority to target
the communications of U.S. persons outside the United States, for the first time ever. It prohibited "reverse targeting," the indirect targeting of U.S. persons' communications via targeting the communications of known terrorists abroad. It also imposed extensive "minimization procedures" that require, among other things, the destruction of much potentially valuable information on U.S. persons, and anyone inside the United States, even before intelligence officials can determine its value. Enormous resources are diverted from actual surveillance to the required paperwork, which includes copious requests for FISA court

orders, and reports and regular briefings to the judiciary and intelligence committees in Congress. Republican calls to fix FISA's structural flaws, principally its outdated distinction between "wire" and "radio" communications, were ignored.

In retrospect, these compromises were worth the trouble because they garnered firm bipartisan support. The great controversy that raged during Bush's second term died down. Sobriety won out over overwrought civil liberties concerns, and the vital national security policies of the post-9/11 world became settled institutions.

Then came the leak of highly classified NSA surveillance programs, and suddenly the debate was raging again. It was now Obama's turn to defend programs that he had previously excoriated Republicans for. Daily security briefings appear to have changed his views.

The Snowden leak has so far involved two distinct programs. The first is the collection of phone records metadata under FISA Section 501 (Section 215 of the Patriot Act). The second is PRISM, which targets the Internet usage of specific foreigners abroad under FISA Section 702, the operative vestige of the Terrorist Surveillance Program. In both cases, the most serious legal and constitutional objections have been exaggerated.

The more intrusive of the two programs is the simpler to dispose. PRISM is just like a phone wiretap except on Internet communications. Like a wiretap, the target is always a specific suspect. But because PRISM's targets are foreigners outside the United States and do not enjoy the protection of the Fourth Amendment's warrant requirements, FISA allows the surveillance to be conducted pursuant to a joint certification of the attorney general and director of national intelligence made to the FISA court on a yearly basis, subject to its approval. That system allows the U.S. government to target specific persons wherever they go (outside the United States). The program should be noncontroversial by now; this is precisely the sort of surveillance that lay at the heart of the FISA Reform Act of 2008, which Congress exhaustively debated for several years. All the objections being raised against it now were raised then, and were either accommodated or rejected with good reason. The program is responsible for foiling about 40 of the 50 terrorist plots which the administration recently disclosed to Congress in classified briefings.

Far more controversy has swirled around the less intrusive of the two programs. Section 215 of the Patriot Act (501 of FISA) allows the government to collect large data sets from phone companies on a daily basis. The data include numbers dialed from, numbers dialed to, length of call, and time of call. The information does not include identity, location, or content.

Critics have assailed the program as a sweeping dragnet, pointing out, for example, that it's easy to identify the owner of a phone number. This criticism misunderstands the nature of the program. It is meant principally to preserve phone record data that the phone companies themselves preserve for long periods of time, and as to which the Supreme Court has ruled there is no expectation of privacy under the Fourth Amendment. The program makes it easier for the government to manipulate and access data that it is already entitled to see without obtaining warrants under various provisions of domestic criminal law.

Under the FISA program, the government can only look up the identity of the person associated with a particular phone number, or otherwise access the data, if it can establish "reasonable articulable suspicion" that the person is involved with some sort of terrorist organization. The suspicion can't be based on speech protected by the First Amendment, such as "I hate Americans." Any data collected are subject to minimization.

Rep. Jim Sensenbrenner, one of the principal authors of the Patriot Act, got a lot of attention recently when he professed shock at the sweep of the program. He claims it goes far beyond the intended scope of Section 215, which is limited to "an investigation to protect against international terrorism or clandestine intelligence activities." But Congress has been briefed on the scope of this program for years, and during that time the 11 judges of the FISA court, sitting individually on a rotating basis, have approved the program every 90 days.

Many libertarian critics have argued that the NSA surveillance violates the Fourth Amendment's prohibition on unreasonable search and seizure. But in fact FISA follows the general progression of safeguards developed elsewhere under Fourth Amendment law. General surveillance can be engaged in routinely without a warrant. Efforts to examine particular data require a showing of probable cause, which demands some clearly articulated reasons for singling out any given person for further scrutiny. Under certain "exigent circumstances," officials can act without a warrant for a period of days, subject to FISA court review. But when targeting U.S. persons anywhere in the world, or anyone inside the United States, whether here legally or not, the government must seek a specific warrant of the FISA court.

The Cato Institute's Julian Sanchez points to the recent case of *U.S.* v. *Jones*, in which the Supreme Court rejected the long-term warrantless tracking of a single vehicle with a GPS device, because, as Justice Samuel Alito wrote in concurrence, law enforcement officers shouldn't be able to "secretly monitor and catalogue every single movement of an individual's car for a very long period." Sanchez argues that such monitoring is even more impermissible when conducted against everybody. He makes the novel case that in the Framers' understanding, " 'unreasonableness' was specifically associated with the absence of particularity—of the kind exhibited by, for instance, an authority to indiscriminately collect all Americans' phone records."

This objection wrongly reads the specificity required for warrants into the general prohibition against unreasonable searches and seizures. It is like saying that police must obtain particular warrants before pointing radar guns at traffic, because otherwise the surveillance is too general, and therefore "unreasonable." This is the same confusion that reigned at the outset of the FISA reform effort, eliding the critical distinction between detection and investigation. Detection is the necessary precursor to an investigation of any particular terrorist pursuant to any sort of warrant. It is necessary in order to develop reasonable suspicion in the first place.

The NSA surveillance is not like the IRS's targeting of conservative groups, as some critics have argued. In the case of the IRS, there are two serious problems: First, the law allows the casual collection of massive amounts of private information on U.S. persons without a warrant; and second, few institutional safeguards protect against abuse by politically motivated officials. In the case of NSA surveillance, by contrast, it is hard to argue convincingly either that the law is too broad or that officials overstepped their bounds.

This latest assault on America's counterterror capabilities will hopefully soon recede, leaving our current legal regime none the worse for wear. But there are reasons to worry. Snowden is apparently travelling with four laptops full of classified information. Worse, the president, in his desire to defend his national security policies, may be tempted to reveal more than is prudent in responding to critics. And the increasing public willingness to extend "whistleblower" legitimacy

to leakers of government secrets could presage a tsunami of security breaches in the months and years ahead.

Addressing the NSA scandals before his trip to the G-8 summit, President Obama said, "If people can't trust not only the executive branch but also don't trust Congress, and don't trust federal judges, to make sure that we're abiding by the Constitution with due process and rule of law, then we're going to have some problems here." Perhaps if he'd given his predecessor more benefit of the doubt on that score, he'd be in a better position to ask for it now. Still, his broader point is inescapably correct. Our system of government is predicated on the idea that because leaders can't always be trusted, the people must be able to place their trust in properly functioning institutions. The difficult question here is whether our institutions have functioned properly, and the most sober answer is yes.

We live in a dangerous world. It is not enough to protect our liberties *from* the power of government. They must also be protected *by* the power of government, from the many enemies who would do us harm. Sensible defenders of civil liberties understand that trade-offs of this sort are both necessary and messy. It is incumbent on us to avoid the allure of treating privacy as an absolute value, on our way to advocating policies that could put us all in danger.

Mario Loyola is former counsel for foreign and defense policy to the Senate Republican Policy Committee and senior fellow at the Texas Public Policy Foundation. Richard A. Epstein is Laurence A. Tisch professor of law at the New York University School of Law, Peter and Kirsten Bedford senior fellow at the Hoover Institution, and senior lecturer at the University of Chicago Law School.