Can a law-abiding liberal democracy be Big Brother?

Jeff Howard explores the legal basis on which the US is collecting vast amounts of data on foreign and US citizens, despite the Fourth Amendment.

It has happened again: seemingly dirty secrets about the conduct of the US government revealed by rogue insiders. In early June 2013, we learned that the National Security Agency (NSA) has been collecting personal records from customers of numerous companies, including Verizon, one of the leading American mobile phone providers. The whistle-blower was Edward Snowden, a 29 year-old security contractor for the NSA and former CIA technician, who told the Guardian: “I have no intention of hiding who I am because I know I have done nothing wrong.”

While many were quick to condemn the discovery of mass data-gathering as illegal, the

government's decision to demand information from Verizon did, in fact, receive judicial permission. On 25 April 2013, a special court known as the Foreign Intelligence Surveillance Court approved a request that Verizon customers' information be handed to the NSA. But on what legal basis could such an apparent invasion of privacy be justified?

FISA, past and future

The legal basis of the data collection goes back, ironically, to a law passed by civil libertarians in the US in 1978. In the aftermath of the Watergate scandal and the discovery of systematic abuses in the executive branch's surveillance operations, Congress passed the Foreign Intelligence Surveillance Act (FISA), aimed at improving oversight of US surveillance operations. By instituting an independent court to review applications for surveillance operations involving US citizens, the bill's supporters (Senator Ted Kennedy and President Jimmy Carter among them) aimed to ensure that U.S. surveillance would comport with the US Constitution's prohibition of "unreasonable searches and seizures" in its Fourth Amendment.

In the aftermath of 9/11, FISA received a facelift courtesy of the Patriot Act. This empowered the government to target individuals unconnected to any particular state. In 2008, Congress passed the FISA Amendments Act—the statute of especial relevance for the latest scandal. The relevant section of the Amendments is Section 702, which empowers the government to collect data on persons it is targeting. While no US citizens (or anyone physically present in the United States) may be legally targeted, data on such persons may legitimately be gathered if they are in contact with persons who are targeted. So, if a suspected terrorist abroad communicates with a US citizen, data on that citizen's records can be collected. By compiling vast quantities of data of this sort, intelligence analysts engage in "link analysis" – a "connect-the-dots" method of identifying particular persons worthy of further investigation and scrutiny in virtue of their communication patterns.

Critics insist that the FISA court is merely a rubber stamp on the basis that it has rejected only 11 applications and approved 20,000 or more in the past 35 years. President Obama has argued that the law is employed with serious discretion, and in any case only permits the gathering of large quantities of data; the government, he insisted, is not actually listening, nor is it permitted to listen, to people's phone calls.

In the eyes of many, such qualified defences are beside the point. Authorising the government to collect vast swathes of data on its own citizens who have contact with suspected terrorists, they say, runs afoul of the Fourth Amendment's prohibition on unreasonable searches. Human rights lawyers took this argument all the way to the Supreme Court. However, the Court ruled that the lawyers lacked legal standing to challenge the case, since they could not demonstrate that they themselves had suffered any concrete invasion of privacy – something that they, by definition, could never demonstrate, since the surveillance is secret.

However, the recent discoveries have prompted the Obama administration to declassify some of its operations, such as the Verizon data-mining programme. This potentially provides an opening for those affected to sue in court — and one such customer, the American Civil Liberties Union, is preparing to do precisely that. Moreover, if the government chooses to grant fresh requests from Google, Microsoft, and Microsoft to release data on the quantity and nature of the specific FISA requests they have received (which they are legally banned from doing), attempts to have either FISA or the specific NSA data-mining programme in question (called “PRISM”) invalidated under the Constitution could be redoubled.

Is FISA beyond the pale?

The mass collection of data on citizens raises serious risks, given what we know about the tendencies of governments to make mistakes and abuse their power. There is a powerful impulse in liberal political thought according to which all surveillance operations — even where restricted to the analysis of mass data — should be shut down. The analogous impulse in American constitutional theory reads the Fourth Amendment as unambiguously condemning such operations as inconsistent with the phrase “no unreasonable searches and seizures.”

But it is not immediately obvious that this impulse is the only reasonable one to adopt. Obama has insisted that these programmes “help us prevent terrorist attacks.” That is not to deny, he argued, that there is no cost in doing this. Trade-offs between privacy and security simply come with the territory if we think — as most people do — that the state should aspire to protect its citizens’ liberty and security. The right to privacy means little if one is under constant threat of a terrorist attack — an insight Thomas Hobbes took seriously when he argued that the state should be able to infringe on any freedoms it wishes so long as such infringements are necessary for keeping citizens safe from attack. But we need not embrace this radical Hobbesian view in order to conclude that the question of FISA’s justifiability is not immediately straightforward on the right balance between liberty and security, even if many do not view it as the most reasonable such balance.

Assuming it is true that FISA is subject to reasonable disagreement, reflecting difficult questions about the proper balance between liberty and security, what is the right response? Our democratic practice already has an answer to the question of how we should decide difficult questions of political morality in the face of reasonable disagreement: we should publicly argue about it, and then vote among the candidate options. This, our practice attests, is the way we respect one another as equals even in the face of our sensible, good faith disagreements. The first response to FISA, then, should not be the knee-jerk one of insisting that the Supreme Court intervene in democratic politics to ban it. Rather, it should be a call to deliberate its merits intelligently and subject it to a democratic vote. It is not clear why reasonable disagreements among conscientiously reasoning citizens should be settled any differently on this matter. Indeed, the aspiration to leave FISA to the people may be what motivated the Supreme Court’s search for a legal technicality that could prevent it from actually addressing FISA’s constitutionality earlier this

year.

The real problem

However, FISA has already been subjected to several democratic votes. It was first passed in 1978, and the 2008 amendments were publicly reauthorised by Congress just a few months ago, with the enthusiastic support of the White House. This takes serious wind out of the sails of opponents who cast FISA as something imposed on them by some autocrat. It has long been known that the government engages in surveillance for the purposes of data-mining under various democratically enacted statutes. It should not have shocked anyone that the government was engaging in this kind of conduct; it flows straightforwardly from Section 702 of the FISA Amendments Act that the state is legally empowered to undertake this sort of surveillance.

Citizens must be more proactive in the pursuit of justice. Those who believe that FISA gets the balance between privacy and security wrong should not wait until a scandal erupts and then cry to the courts for help. They should live up to the demands with which democratic citizenship rightly saddles them, and take responsibility for what laws are passed — and reauthorised — in the first place.

Postscript: abusing reasonable legislation

Since writing the original post, it has become clear that the National Security Agency has engaged in activity of questionable constitutional status. Even if we should believe, as I have argued, that FISA is a reasonable (if not uniquely reasonable) solution to the question of how to balance liberty and security, that does not mean that it is immune from being stretched, distorted, and even ignored. Yet this is precisely what the National Security Agency has done in some cases. Two particular issues stand out as worthy of keeping in mind.

Firstly, the National Security Agency has violated standards of privacy that protect persons on American territory 2,776 times. In many cases, this was the outcome of an insufficiently subtle and responsive data collection system. One of the most important failures concerned persons abroad whose mobile phones were under surveillance but who then entered the U.S.—a fact that triggers the necessity of a warrant, which in 1,904 cases was never sought nor granted. This episode raises the question: are the technological hurdles to conducting surveillance legally so onerous that such surveillance is best not undertaken in the first place? The NSA has failed to answer this question adequately.

Secondly, the National Security Agency has engaged in the practice of electronically copying all emails exchanged between Americans and persons abroad. As Alexander Abdo and Patrick Toomey made the point: “If you [in the U.S.] emailed a friend, family member or colleague overseas today (or if, from abroad, you emailed someone in the US), chances are that the NSA made a copy of that email and searched it for suspicious information.” Importantly, the emails

ultimately read are not simply those in which the sender or recipient is a suspected terrorist. If an email simply mentions a particular keyword, like an al-Qaeda agent's name—as an email exchange between two international relations scholars, or a son and his father, or a lawyer and his client, could obviously do—it is examined without a warrant by the National Security Agency. Most emails are putatively deleted once a search is not found; but it is not clear that a search deemed unreasonable by the Fourth Amendment could suddenly become reasonable simply because it is accomplished using breathtakingly fast, secret technology.

As the case for the U.S. government's moral incompetence in these cases becomes greater, the reasonableness of assigning the NSA secret surveillance powers becomes more and more questionable. Our determinations of what is reasonable rightly shift in response to evidence about what sorts of methods and institutions are morally reliable and which are not. That is not to say that all of what the NSA does is morally illegitimate. Their efforts have undoubtedly saved many lives. But we must be certain that in aspiring to protect a free society from assault by its enemies, we do not compromise the elements of such a society that make it worth protecting in the first place.

Jeffrey Howard recently completed his doctorate in political theory at Nuffield College, Oxford. From 1 September 2013, he will take up a faculty position as Lecturer in Political Theory in the Department of Government at the University of Essex.

Published on:July 3, 2013