Connecticut Debate Association

Novice Scrimmage, September 28, 2013

St. Luke's School and Xavier High School

Resolved: The US should not prosecute Edward Snowden.

Edward Snowden: Traitor, whistleblower or defector?

By Lindsey Boerma, CBS News/ August 12, 2013, 6:00 AM

The United States has "poisoned the well, so to speak" for Edward Snowden's chances of receiving a fair trial, his father worried Sunday, shortly after declaring he has secured travel documents to visit his son in Russia, where he has taken asylum.

"As a father, I want my son to come home if I believe that the justice system... is going to be applied correctly," Lon Snowden said on ABC's "This Week." Federal prosecutors have filed three criminal complaints against Edward Snowden - two of which were brought under the Espionage Act - for leaking information in May about top-secret National Security Agency programs designed to track potential terrorist activity by culling metadata from U.S. citizens.

During his trip, the elder Snowden said he plans to convey to his son that he's "not open" to a plea deal with U.S. authorities. He cited his doubts that the "absolutely irresponsible" descriptions of Edward's actions by lawmakers and President Obama's administration would not sway a future jury.

Stateside, though, U.S. officials seem uncertain how to even classify Snowden. "Traitor" was the favorite in the immediate, fiery aftermath of his revelations - brandished by everyone from Secretary of State John Kerry to House Speaker John Boehner, R-Ohio. But it wasn't fired once on this week's Sunday show circuit.

Appearing on CBS News' "Face the Nation," Gen. Michael Hayden - former CIA and NSA director - while defending the NSA programs as being effective and legally sound, argued: "Traitor is narrowly defined in the Constitution. ...We used to have a word for somebody who stole our secrets, who got the job to steal our secrets, and then he moved with those secrets to a foreign country, and made those secrets public. It wasn't a whistleblower; it was defector. And I actually think that's a very good word for him."

But that term, "whistleblower," has been wielded since the beginning by Snowden supporters like Wikileaks founder Julian Assange, who remains holed up in fear of extradition over his own release of classified U.S. documents. This weekend, Assange trumpeted what he perceived to be concession by the president that Snowden indeed fits the "whistleblower" mold.

Mr. Obama on Friday laid out a series of steps to reform NSA transparency and oversight - and in the same breath, preempted the idea that Snowden single-handedly jumpstarted debate over government surveillance. "I called for a thorough review of our surveillance operations before Mr. Snowden made these leaks," he said. "My preference - and I think the American people's preference - would have been for a lawful, orderly examination of these laws; a thoughtful, fact-based debate."

Assange in a statement scoffed at that assessment, opining that "the President and people of the United States and around the world owe Edward Snowden a debt of gratitude" because "without Snowden's disclosures, no one would know about the programs and no reforms could take place. ...His biggest concern was if he blew the whistle and chance did not occur. Well, reforms are taking shape."

Hayden on Sunday tried to bolster the president's point, arguing that "clearly," the debate about government surveillance overreach "was coming," and Snowden acted simply as a catalyst.

Snowden, he said, "accelerated it; he didn't inform it. He made it more emotional. And so, you know, there are some real downsides to what he's done. I'll give you an example. You and I witnessed Katrina, right? I'm telling you right now... the levees around Lake Pontchartrain are the strongest they've been in a century, but Katrina was still a bad thing and that's how I view Mr. Snowden."

One GOP lawmaker, though, rallied to Assange's side, saying the president wouldn't have rolled out "window dressing" reforms to lawful, working surveillance programs had it not been for Snowden.

"I think Snowden came out, leaked this information, and the White House has been backtracking ever since," House

Homeland Security Committee Chairman Mike McCaul, R-Texas, said on NBC's "Meet the Press." "The problem fundamentally is he's failed to explain these programs, which are lawful, which have saved lives, which have stopped terrorist plots. He has not adequately defended them.

"And now he's in a bit of a mess," McCaul continued, "because on the heels of the IRS scandal, where peopled don't trust this government, this administration, with their tax records, they sure don't trust this administration with their phone records."

Rep. Peter King, R-N.Y., a member of the House Intelligence Committee, agreed on "Face the Nation" the president's primary fault has been staying "silent for the past two months."

"He allowed the Edward Snowdens and others in the world to dominate the media, and now we have people thinking the NSA is spying on people, is listening to our phone calls," he said. "The president of the United States as commander-in-chief had the obligation to be aggressively and effectively defending his program, and he really didn't do it."

The top Democrat on the House Intelligence Committee, Rep. Dutch Ruppersberger, D-Md., offered up his own take on Snowden, which he said "speaks for itself": "When you work for the intelligence community, first thing you take an oath not to violate classified information. This individual now has said that he went in for the purpose of getting information. He turned his back on his country and where did he go once he got this information? He went to China and then he went to Russia."

Still, though the NSA surveillance methods in no way violate Americans' privacy, Ruppersberger qualified, with details of the programs circulating internationally thanks to Snowden, reforms may be necessary, if only to placate public perception.

"We in politics have to deal with perception, not just reality," he said. "And we need to do better in educating our public so they are not fearful that we, the government, are violating their privacy - that's very important."

Is NSA Leaker Edward Snowden a Traitor?

by Andre de Nesnera, Voice of America, August 8, 2013

The White House has cancelled a planned summit meeting next month between President Barack Obama and Russian President Vladimir Putin and one of the reasons given was Moscow's decision to grant asylum to an American who leaked top secret information.

The American, former intelligence contractor Edward Snowden, is wanted in the United States on espionage charges after he leaked information about how the super-secret National Security Agency (NSA) monitors U.S. and international telephone and Internet traffic.

Snowden is now living in Russia after spending more than a month in the transit area of a Moscow airport. But his plight has triggered a discussion on the issue of treason.

In other words, is Snowden a traitor?

For John Bolton, former U.S. Ambassador to the United Nations, the issue is clear.

"I do consider him a traitor. He has taken vital secrets of the United States, undoubtedly given some to China, given some to Russia — Russia and China may have them all now for what we know," Bolton told VOA.

"Some people say well that's not really espionage, because espionage only takes place when you give it to one government," Bolton continued. "I'd have to say making it public is worse than espionage, because then you have 190 governments that learn America's secrets."

David Barrett, a national security expert teaching at Villanova University, sees Snowden in a different light.

"I would regard him as a defector. There are a lot of different names that are used to describe him: whistleblower, leaker," Barrett said. "Sure, I'd call him a defector. This is a very serious event for a person who works for an intelligence agency, who signs documents agreeing to keep things secret. I think it is a very serious thing to reveal those secrets – to leave this country and reveal these secrets."

Defector, traitor or whistleblower?

The U.S. Justice Department has filed criminal charges against Snowden — theft of government property, unauthorized communication of national defense information and willful communication of classified communications intelligence to an unauthorized person.

Snowden tries to justify his actions by saying one of the reasons he leaked the documents was to start a discussion about the U.S. government's secret spying programs.

Stephen Vladeck, an expert on national security law at American University College of Law, says those discussions would not be happening now if it weren't for Snowden's action.

"I think it's a good thing that they are happening," he said. "At the end of the day, if someone asks me 'is Edward Snowden a criminal or a whistleblower,' I would say 'yes' — he's both. And that's okay.

"And that goes to the larger point that we have to keep in mind that sometimes doing what's legal and doing what's right are not necessarily the same thing," said Vladeck.

Precise definition

Aziz Huq, an expert on national security issues and constitutional law at the University of Chicago, says one thing is for sure: Edward Snowden is not a traitor.

"We have a very precise definition of treason in American law," Huq said. "And it's a definition that is embedded, not just in a federal statute; it is actually embedded in the Constitution. And it refers to a very narrow class of 'intentional forms of aiding an enemy in times of war.'"

For example, says Huq, those Americans who fought with the Nazi army were traitors — and there were treason prosecutions and executions in World War II.

"The last person who was indicted for treason, a chap named Adam Gadahn, who is an American, who went to join al-Qaida and serve as one of their English language spokesperson — there is a very strong argument for indicting him under the treason statute because he has gone and aided, in an affirmative and intentional way, an enemy of the United States. Those conditions and those cases are nothing like Snowden's case."

Huq says there is something "extraordinarily inappropriate about using the word 'traitor' with respect to somebody who has disclosed information that is unquestionably relevant to the public debate."

A majority of Americans seem to agree with Huq. A recent Quinnipiac University poll says 55 percent of those questioned believe Snowden is a whistleblower, but not a traitor.

http://www.voanews.com/content/snowden-traitor/1726272.html

Edward Snowden is a Whistleblower

By Michael German, Senior Policy Counsel, ACLU Washington Legislative Office, Aug 2, 2013

This piece originally ran at the ACSblog.

My American Civil Liberties Union colleagues and I have been extremely busy since the Guardian and the Washington Post published leaked classified documents exposing the scope of the government's secret interpretations of the Patriot Act and the 2008 amendments to the Foreign Intelligence Surveillance Act, which allow the FBI and NSA to spy on hundreds of millions of innocent Americans. We haven't written much about the alleged leaker of this information, Edward Snowden, however, mainly because we took his advice to focus on what the NSA and FBI were doing, rather than on what he did or didn't do. (See exceptions here and here).

But I did want to clear up a question that seems to keep coming up: whether Snowden is a whistleblower. It is actually not a hard question to answer. The Whistleblower Protection Act protects "any disclosure" that a covered employee reasonably believes evidences "any violation of any law, rule, or regulation," or "gross mismanagement, a gross waste of funds, and abuse of authority, or a substantial and specific danger to public health or safety."

In the two months since Snowden's alleged disclosures, no fewer than five lawsuits have been filed challenging the legality of the surveillance programs he exposed. The author of the Patriot Act, Rep. James Sensenbrenner (R-Wis.), called the scope of data collection revealed in one of the leaked Foreign Intelligence Surveillance Court orders "incredibly troubling," and "an overbroad interpretation of the Act" that "raise[s] questions about whether our constitutional rights are secure."

It doesn't end there. Over a dozen bills have been introduced in Congress to narrow these now public surveillance authorities and increase transparency regarding continuing programs. No one can know what was in Edward Snowden's mind, but clearly he could have had a reasonable belief the documents he leaked to the news media revealed government illegality and abuse of authority.

The disclosures also revealed that U.S. military officers and intelligence community officials have been less than truthful in their public comments and congressional testimony about the government's domestic surveillance practices, both in the scope of the programs and their effectiveness. Such false and misleading testimony threatens

more than just Americans' privacy; it threatens democratic control of government.

Americans need and deserve truthful information about what the government is doing, particularly where the activity infringes on individual rights. As the father of the Constitution James Madison said, "A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both." Denying Americans this knowledge through excessive and unnecessary secrecy, or worse, official deception, is unjustifiable and illegal. In a democracy, the law should never be secret.

The countless articles on the front pages of dozens of newspapers across the country since the documents leaked reveal the public thirst for this information. It is clear that these disclosures benefited the public, by giving victims of illegal surveillance – essentially all Americans – the knowledge and opportunity to challenge these unconstitutional programs, both in the courts and through their elected representatives in Congress. Even President Obama said he "welcomed this debate" and thought it was "healthy for our democracy." Yet a properly informed public debate on these programs would not have been possible without Snowden's leaks.

But the fact that the leaks served the public interest by exposing government illegality and abuse doesn't mean Snowden is protected by the law, because the intelligence community has always been exempted from the Whistleblower Protection Act. This fact refutes the other common misperception: that there are effective internal avenues for reporting illegal activities within the intelligence community.

Congress passed the Intelligence Community Whistleblower Protection Act in 1998, but it is no more than a trap. It establishes a procedure for internal reporting within the agencies and through the Inspector General to the congressional intelligence committees, but it provides no remedy for reprisals that occur as a result. Reporting internally through the ICWPA only identifies the whistleblowers, leaving them vulnerable to retaliation. The examples of former NSA official Thomas Drake, former House Intelligence Committee staffer Diane Roark and former CIA officer Sabrina De Sousa show too well.

This lack of protection means that when intelligence community employees and contractors – who take an oath to defend the Constitution – see government illegality they must turn the other way, or risk their careers and possibly even their freedom. The people we trust to protect our nation from foreign enemies deserve legal protection when they blow the whistle on wrongdoing within government.

Michael German is senior policy counsel at the ACLU's Washington Legislative Office and a former FBI agent.

Americans Have Completely Flipped On Edward Snowden In The Past Month

By Brett LoGiurato, Business Insider, Jul. 24, 2013, 8:58 AM 8,069 77

The American public's views of National Security Agency leak source Edward Snowden have flipped in the past month, according to one poll — and now most support him being charged with a crime.

According to the ABC-Washington Post poll, 53% say that Snowden should be charged with a crime after exposing a trove of NSA secrets, compared with 36% who disagree. That's a sharp turn from the point immediately after his revelations in June, when Americans opposed him being charged by a 48-43 margin.

Snowden is currently in Russia, where he is reportedly being allowed to leave the Moscow airport transit zone in which he has been stationed for the past month. His lawyer said he plans to stay in Russia and attempt to start a life there — meaning the public's views of him probably won't improve.

According to the ABC-WaPo poll, 57% of Americans believe that it is more important for the NSA to "investigate possible terrorist threats, even if that intrudes on personal privacy" — the Obama administration's justification for the programs. Only 39% think it's more important for the government not to intrude on personal privacy, "even if that limits its ability to investigate possible terrorist threats."

It's worth noting that other polls, worded differently, have produced different results. A Quinnipiac poll released earlier this month showed that there had been a "massive swing" in views on government surveillance in the aftermath of Snowden's leaks.

The Solitary Leaker

By DAVID BROOKS, The New York Times, June 10, 2013

From what we know so far, Edward Snowden appears to be the ultimate unmediated man. Though obviously terrifically bright, he could not successfully work his way through the institution of high school. Then he failed to

navigate his way through community college.

According to The Washington Post, he has not been a regular presence around his mother's house for years. When a neighbor in Hawaii tried to introduce himself, Snowden cut him off and made it clear he wanted no neighborly relationships. He went to work for Booz Allen Hamilton and the C.I.A., but he has separated himself from them, too.

Though thoughtful, morally engaged and deeply committed to his beliefs, he appears to be a product of one of the more unfortunate trends of the age: the atomization of society, the loosening of social bonds, the apparently growing share of young men in their 20s who are living technological existences in the fuzzy land between their childhood institutions and adult family commitments.

If you live a life unshaped by the mediating institutions of civil society, perhaps it makes sense to see the world a certain way: Life is not embedded in a series of gently gradated authoritative structures: family, neighborhood, religious group, state, nation and world. Instead, it's just the solitary naked individual and the gigantic and menacing state.

This lens makes you more likely to share the distinct strands of libertarianism that are blossoming in this fragmenting age: the deep suspicion of authority, the strong belief that hierarchies and organizations are suspect, the fervent devotion to transparency, the assumption that individual preference should be supreme. You're more likely to donate to the Ron Paul for president campaign, as Snowden did.

It's logical, given this background and mind-set, that Snowden would sacrifice his career to expose data mining procedures of the National Security Agency. Even if he has not been able to point to any specific abuses, he was bound to be horrified by the confidentiality endemic to military and intelligence activities. And, of course, he's right that the procedures he's unveiled could lend themselves to abuse in the future.

But Big Brother is not the only danger facing the country. Another is the rising tide of distrust, the corrosive spread of cynicism, the fraying of the social fabric and the rise of people who are so individualistic in their outlook that they have no real understanding of how to knit others together and look after the common good.

This is not a danger Snowden is addressing. In fact, he is making everything worse.

For society to function well, there have to be basic levels of trust and cooperation, a respect for institutions and deference to common procedures. By deciding to unilaterally leak secret N.S.A. documents, Snowden has betrayed all of these things.

He betrayed honesty and integrity, the foundation of all cooperative activity. He made explicit and implicit oaths to respect the secrecy of the information with which he was entrusted. He betrayed his oaths.

He betrayed his friends. Anybody who worked with him will be suspect. Young people in positions like that will no longer be trusted with responsibility for fear that they will turn into another Snowden.

He betrayed his employers. Booz Allen and the C.I.A. took a high-school dropout and offered him positions with lavish salaries. He is violating the honor codes of all those who enabled him to rise.

He betrayed the cause of open government. Every time there is a leak like this, the powers that be close the circle of trust a little tighter. They limit debate a little more.

He betrayed the privacy of us all. If federal security agencies can't do vast data sweeps, they will inevitably revert to the older, more intrusive eavesdropping methods.

He betrayed the Constitution. The founders did not create the United States so that some solitary 29-year-old could make unilateral decisions about what should be exposed. Snowden self-indulgently short-circuited the democratic structures of accountability, putting his own preferences above everything else.

Snowden faced a moral dilemma. On the one hand, he had information about a program he thought was truly menacing. On the other hand, he had made certain commitments as a public servant, as a member of an organization, and a nation. Sometimes leakers have to leak. The information they possess is so grave that it demands they violate their oaths.

But before they do, you hope they will interrogate themselves closely and force themselves to confront various barriers of resistance. Is the information so grave that it's worth betraying an oath, circumventing the established decision-making procedures, unilaterally exposing secrets that can never be reclassified?

Judging by his comments reported in the news media so far, Snowden was obsessed with the danger of data mining but completely oblivious to his betrayals and toward the damage he has done to social arrangements and the invisible bonds that hold them together.

Politics & Ideas: How Much Transparency Do We Really Want?

By William A. Galston, 21 August 2013, The Wall Street Journal

The controversy over NSA surveillance raises two distinct issues -- privacy and transparency -- that are often conflated. Privacy in today's world denotes a right or expectation that individuals are entitled to keep certain matters to themselves unless they have consented to disclose them, or unless there is a compelling justification for their disclosure. In this sense, privacy and opacity go together.

Many Americans believed that the equivalent of a wall protected their email and telephone communications from government intrusion, only to learn that they were living in a virtual glass house. That these disclosures have set off shock and dismay should come as no surprise.

Transparency is very nearly the opposite of privacy. In the current controversy, it is a demand that the government make public matters it conducts in private and wants to keep private.

The argument for disclosure goes like this: If the government is acting in the name of the people, the people need to know what their government is doing. How else can they judge these activities? Democratic government means accountability to the public, and accountability requires disclosure. History testifies to the link between secrecy and the abuse of public power. Without disclosure, the people will find it difficult to restrain government's excesses -- most importantly, secret activities that could endanger our liberties.

Government transparency has a distinguished history. In 1795, Immanuel Kant propounded what is often called the principle of publicity: Roughly, if you cannot reveal the principle that guides your policy without undermining that policy, then the policy itself is fatally flawed from a moral point of view.

Little more than a century later, in his famous "Fourteen Points" speech about U.S. war aims and the principles that would guide the peace, President Woodrow Wilson called for "Open covenants of peace, openly arrived at, after which there shall be no private international understandings of any kind but diplomacy shall proceed always frankly and in the public view."

The problem here is obvious: Policy makers often face a choice between private diplomacy and no diplomacy. Secretary of State John Kerry clearly thought that the precise content of his shuttle diplomacy between Israel and the Palestinian Authority had to be kept from public view if there was to be any chance of restarting peace talks. A measure of secrecy is a necessary (if not sufficient) condition of success.

This maxim applies broadly. No one thinks that nations at war have a responsibility to make their military strategy public. If the Allies had not succeeded in confusing the Germans, the Normandy landing might have failed.

The same consideration of secrecy applies to the acquisition of intelligence. Government officials believe that revealing the details, or even the existence, of secret surveillance programs would help our adversaries elude their reach. They also believe that briefing more than a handful of elected representatives would lead inevitably to public disclosure. Those who do receive briefings are sworn not to reveal their substance, even in congressional debate.

Effectiveness and accountability collide -- a tension that can be managed more or less well but never entirely abolished.

In the wake of Vietnam and Watergate, Congress and the executive branch pieced together a new strategy for managing this tension. Institutions such as congressional intelligence committees and the Foreign Intelligence Surveillance Court would ensure executive branch accountability while preserving necessary secrecy.

The current surveillance controversy challenges the entire post-Watergate regime. Many members of Congress have come to doubt that the intelligence committees permit sufficient accountability; an increasing share of the public now doubts that the system established by the 1978 Foreign Intelligence Surveillance Act adequately protects privacy.

But what is to replace it? If secrecy is diminished in the name of public accountability and individual liberty, are we willing to sacrifice a measure of security?

Yet the relation between collective security and individual liberty is not zero-sum. Because another 9/11-scale terrorist event might well lead to even more intrusive antiterrorism measures, reducing the likelihood of such an event could end up preventing serious infringements on liberty. Up to a point, liberty and security can be mutually reinforcing. But at what point do they become opposed?

This is not a judgment that can be left to experts in the executive branch. Ultimately, the people, acting through their elected representatives, must decide -- and it is hard to see how they can do so unless all representatives, not just a select few, have the information they need to participate in such a decision.

As we learned in the 1970s, however, public deliberation on intelligence matters is anything but cost-free.

Stop Freaking Out About the NSA: The government's phone surveillance isn't Orwellian. It's limited and supervised.

By William Saletan|Posted Thursday, June 6, 2013, at 3:52 PM, Slate, Frame Game

You don't need a wiretap to hear what people are saying about the National Security Agency's phone surveillance program. The program's details, disclosed in a secret court order leaked to the Guardian, show that at least one major company, Verizon, has been legally required to give the government information about its subscribers' communications. "An astounding assault on the Constitution," says Rand Paul. "Obscenely outrageous," says Al Gore. "Beyond Orwellian," says the ACLU.

Chill. You can quarrel with this program, but it isn't Orwellian. It's limited, and it's controlled by checks and balances.

The program's purpose, according to administration officials and knowledgeable members of Congress, is to find out who's been calling or receiving calls from phone numbers linked to known or suspected terrorists. If Tamerlan Tsarnaev had been in contact with somebody flagged as a possible jihadist operative, this is the kind of surveillance that would have brought him to the attention of counterterrorism investigators, even without Russian assistance.

The leaked order is certainly worth discussing. It confirms that previous lines have been crossed. It's now clear that the surveillance program, which was known to have been conducted under President Bush, has continued under President Obama. Moreover, there's no requirement that at least one party to the call must be foreign. The order includes calls "wholly within the United States." Nor is there any requirement that the government show probable cause to justify its demand for any particular record. It only has to offer "reasonable grounds to believe" that the records being sought are "relevant to an authorized investigation."

But the program is also restrained in several ways. Here's a list.

1. It isn't wiretapping. The order authorizes the transfer of "telephony metadata" such as the date and length of each call and which phone numbers were involved. It doesn't include the content of calls—which is more tightly protected by the Fourth Amendment—or the identity of the callers. The targeted data are mathematical, not verbal. They're the kind of information you'd request if you were mapping possible extensions of a terrorist or criminal network.

2. It's judicially supervised. The leaked document is a court order. It was issued by the Foreign Intelligence Surveillance [FISA] Court. To get the Verizon data, the FBI had to ask the court for permission. The Bush administration used to extract this kind of metadata unilaterally. The Obama administration has changed the rules to bring in the court as an overseer.

3. It's congressionally supervised. Any senator who's expressing shock about the program is a liar or a fool. The Senate Intelligence and Judiciary Committees have been briefed on it many times. Committee members have had access to the relevant FISA court orders and opinions. The intelligence committee has also informed all senators in writing about the program, twice, with invitations to review classified documents about it prior to reauthorization. If they didn't know about it, they weren't paying attention.

4. It expires quickly unless it's reauthorized. The leaked order was issued on April 25 and expires on July 19. That's the way these orders have worked for years: The court has to review and reapprove the surveillance request, or the authority to transfer the records expires.

5. Wiretaps would require further court orders. The reason the leaked order is so broad is that it applies only to metadata. If, after looking at its map of phone numbers, the government decides that yours might belong to a potential terrorist, it can seek further information, including the content of your calls. But in that case, it has to ask the court for a separate order, which in turn would require enough evidence to override your Fourth Amendment rights.

Is government surveillance worth worrying about? Sure. But even broad surveillance, per se, isn't outrageous. What's important is that the surveillance be warranted by real threats, appropriately limited, and supervised by competing branches of government. In this case, those standards have been met.

People v. NSA: Who represents the public at the Foreign Intelligence Surveillance Court?

By Brian Palmer|Posted Thursday, June 6, 2013, at 4:01 PM, Slate, Explainer

The National Security Agency is collecting metadata on the calls of all Verizon customers according to a report from the Guardian. Obama administration officials have defended their surveillance activities, without admitting to anything specific, noting that the Foreign Intelligence Surveillance Court approves such intelligence gathering. Who represents the privacy interests of ordinary Americans before the secret intelligence court?

No one. Applications for surveillance orders from the FISA court are nonadversarial, which means the target of the investigation is not represented. The judges, working on their own, are supposed to ensure that the government meets the legal standard. In practice, there's little the judges can do to stop investigators from getting what they want because the standard is so low. The government must show that it seeks information "relevant to an authorized investigation." Relevance is presumed if the government merely states—not proves—that the records relate to: "(1) a foreign power or an agent of a foreign power; (2) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation." Absent congressional action, it's very unlikely you'll have representation before the FISA court anytime soon. Last year, the Supreme Court ruled that a group of journalists and attorneys lacked standing to challenge the procedures because they couldn't prove any injury to themselves.

Although you had no opportunity to contest the order that delivered your phone data to the NSA, Verizon likely had some say. After a surveillance order is issued, electronic service providers may present a challenge if they feel the order is impractical or overly burdensome.

The government has an astonishing success rate before the FISA court. Between 2010 and 2012, the court approved all of the 5,180 applications for surveillance and physical searches except for one that the government unilaterally withdrew. Despite receiving more than a 1,000 requests every year since 2002, the court has never denied more than four applications in a single year.

Those statistics may be slightly unfair to the judges, though. Former FISA court judges claim that they sometimes persuade government investigators to modify or narrow their requests before issuing the approval. In 2012, the judges modified 39 orders out of 1,856. The government must also submit "minimization procedures" along with the application, which are supposed to prevent the misuse of information belonging to innocent people. However, as with other aspects of foreign intelligence gathering, it's difficult to ascertain whether the government is complying with its own minimization procedures.

The current makeup of the FISA court is probably favorable to approvals. The 11 judges on the lower level of the court and the three appellate judges are appointed by the chief justice of the United States. Since the FISA court was established in 1978, every chief justice has been a Republican appointee with a fairly broad view of the government's powers in safeguarding national security.

Got a question about today's news? Ask the Explainer.

Explainer thanks Stephen I. Vladeck of American University Washington College of Law, who blogs on national security law at Lawfare.

The Banality of Systemic Evil

By PETER LUDLOW, The New York Times, September 15, 2013

In recent months there has been a visible struggle in the media to come to grips with the leaking, whistle-blowing and hacktivism that has vexed the United States military and the private and government intelligence communities. This response has run the gamut. It has involved attempts to condemn, support, demonize, psychoanalyze and in some cases canonize figures like Aaron Swartz, Jeremy Hammond, Chelsea Manning and Edward Snowden.

In broad terms, commentators in the mainstream and corporate media have tended to assume that all of these actors needed to be brought to justice, while independent players on the Internet and elsewhere have been much more supportive. Tellingly, a recent Time magazine cover story has pointed out a marked generational difference in how people view these matters: 70 percent of those age 18 to 34 sampled in a poll said they believed that Snowden "did a good thing" in leaking the news of the National Security Agency's surveillance program.

So has the younger generation lost its moral compass?

No. In my view, just the opposite.

Clearly, there is a moral principle at work in the actions of the leakers, whistle-blowers and hacktivists and those

who support them. I would also argue that that moral principle has been clearly articulated, and it may just save us from a dystopian future.

In "Eichmann in Jerusalem," one of the most poignant and important works of 20th-century philosophy, Hannah Arendt made an observation about what she called "the banality of evil." One interpretation of this holds that it was not an observation about what a regular guy Adolf Eichmann seemed to be, but rather a statement about what happens when people play their "proper" roles within a system, following prescribed conduct with respect to that system, while remaining blind to the moral consequences of what the system was doing — or at least compartmentalizing and ignoring those consequences.

A good illustration of this phenomenon appears in "Moral Mazes," a book by the sociologist Robert Jackall that explored the ethics of decision making within several corporate bureaucracies. In it, Jackall made several observations that dovetailed with those of Arendt. The mid-level managers that he spoke with were not "evil" people in their everyday lives, but in the context of their jobs, they had a separate moral code altogether, what Jackall calls the "fundamental rules of corporate life":

(1) You never go around your boss. (2) You tell your boss what he wants to hear, even when your boss claims that he wants dissenting views. (3) If your boss wants something dropped, you drop it. (4) You are sensitive to your boss's wishes so that you anticipate what he wants; you don't force him, in other words, to act as a boss. (5) Your job is not to report something that your boss does not want reported, but rather to cover it up. You do your job and you keep your mouth shut.

Jackall went through case after case in which managers violated this code and were drummed out of a business (for example, for reporting wrongdoing in the cleanup at the Three Mile Island nuclear power plant).

Aaron Swartz counted "Moral Mazes" among his "very favorite books." Swartz was the Internet wunderkind who was hounded by a government prosecution threatening him with 35 years in jail for illicitly downloading academic journals that were behind a pay wall. Swartz, who committed suicide in January at age 26 (many believe because of his prosecution), said that "Moral Mazes" did an excellent job of "explaining how so many well-intentioned people can end up committing so much evil."

Swartz argued that it was sometimes necessary to break the rules that required obedience to the system in order to avoid systemic evil. In Swartz's case the system was not a corporation but a system for the dissemination of bottled up knowledge that should have been available to all. Swartz engaged in an act of civil disobedience to liberate that knowledge, arguing that "there is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture."

Chelsea Manning, the United States Army private incarcerated for leaking classified documents from the Departments of Defense and State, felt a similar pull to resist the internal rules of the bureaucracy. In a statement at her trial she described a case where she felt this was necessary. In February 2010, she received a report of an event in which the Iraqi Federal Police had detained 15 people for printing "anti-Iraqi" literature. Upon investigating the matter, Manning discovered that none of the 15 had previous ties to anti-Iraqi actions or suspected terrorist organizations. Manning had the allegedly anti-Iraqi literature translated and found that, contrary to what the federal police had said, the published literature in question "detailed corruption within the cabinet of Prime Minister Nuri Kamal al-Maliki's government and the financial impact of his corruption on the Iraqi people."

When Manning reported this discrepancy to the officer in charge (OIC), she was told to "drop it," she recounted.

Manning could not play along. As she put it, she knew if she "continued to assist the Baghdad Federal Police in identifying the political opponents of Prime Minister al-Maliki, those people would be arrested and in the custody of the Special Unit of the Baghdad Federal Police and very likely tortured and not seen again for a very long time — if ever." When her superiors would not address the problem, she was compelled to pass this information on to WikiLeaks.

Snowden too felt that, confronting what was clearly wrong, he could not play his proper role within the bureaucracy of the intelligence community. As he put it,

[W]hen you talk to people about [abuses] in a place like this where this is the normal state of business people tend not to take them very seriously and move on from them. But over time that awareness of wrongdoing sort of builds up and you feel compelled to talk about [them]. And the more you talk about [them] the more you're ignored. The more you're told it's not a problem until eventually you realize that these things need to be determined by the public and not by somebody who was simply hired by the government.

The bureaucracy was telling him to shut up and move on (in accord with the five rules in "Moral Mazes"), but Snowden felt that doing so was morally wrong.

In a June Op-Ed in The Times, David Brooks made a case for why he thought Snowden was wrong to leak information about the Prism surveillance program. His reasoning cleanly framed the alternative to the moral code endorsed by Swartz, Manning and Snowden. "For society to function well," he wrote, "there have to be basic levels of trust and cooperation, a respect for institutions and deference to common procedures. By deciding to unilaterally leak secret N.S.A. documents, Snowden has betrayed all of these things."

The complaint is eerily parallel to one from a case discussed in "Moral Mazes," where an accountant was dismissed because he insisted on reporting "irregular payments, doctored invoices, and shuffling numbers." The complaint against the accountant by the other managers of his company was that "by insisting on his own moral purity … he eroded the fundamental trust and understanding that makes cooperative managerial work possible."

But wasn't there arrogance or hubris in Snowden's and Manning's decisions to leak the documents? After all, weren't there established procedures determining what was right further up the organizational chart? Weren't these ethical decisions better left to someone with a higher pay grade? The former United States ambassador to the United Nations, John Bolton, argued that Snowden "thinks he's smarter and has a higher morality than the rest of us … that he can see clearer than other 299, 999, 999 of us, and therefore he can do what he wants. I say that is the worst form of treason."

For the leaker and whistleblower the answer to Bolton is that there can be no expectation that the system will act morally of its own accord. Systems are optimized for their own survival and preventing the system from doing evil may well require breaking with organizational niceties, protocols or laws. It requires stepping outside of one's assigned organizational role. The chief executive is not in a better position to recognize systemic evil than is a middle level manager or, for that matter, an IT contractor. Recognizing systemic evil does not require rank or intelligence, just honesty of vision.

Persons of conscience who step outside their assigned organizational roles are not new. There are many famous earlier examples, including Daniel Ellsberg (the Pentagon Papers), John Kiriakou (of the Central Intelligence Agency) and several former N.S.A. employees, who blew the whistle on what they saw as an unconstitutional and immoral surveillance program (William Binney, Russ Tice and Thomas Drake, for example). But it seems that we are witnessing a new generation of whistleblowers and leakers, which we might call generation W (for the generation that came of age in the era WikiLeaks, and now the war on whistleblowing).

The media's desire to psychoanalyze members of generation W is natural enough. They want to know why these people are acting in a way that they, members of the corporate media, would not. But sauce for the goose is sauce for the gander; if there are psychological motivations for whistleblowing, leaking and hacktivism, there are likewise psychological motivations for closing ranks with the power structure within a system — in this case a system in which corporate media plays an important role. Similarly it is possible that the system itself is sick, even though the actors within the organization are behaving in accord with organizational etiquette and respecting the internal bonds of trust.

Just as Hannah Arendt saw that the combined action of loyal managers can give rise to unspeakable systemic evil, so too generation W has seen that complicity within the surveillance state can give rise to evil as well — not the horrific evil that Eichmann's bureaucratic efficiency brought us, but still an Orwellian future that must be avoided at all costs.

Peter Ludlow is a professor of philosophy at Northwestern University and writes frequently on digital culture, hacktivism and the surveillance state.