Time Magazine

Monday, Jun. 24, 2013

The Geeks Who Leak

By Michael Scherer

Correction Appended: June 13, 2013

The 21st century mole demands no payments for his secrets. He sees himself instead as an idealist, a believer in individual sovereignty and freedom from tyranny. Chinese and Russian spooks will not tempt him. Rather, it's the bits and bytes of an online political philosophy that attract his imagination, a hacker mentality founded on message boards in the 1980s, honed in chat rooms in the '90s and matured in recent online neighborhoods like Reddit and 4chan. He believes above all that information wants to be free, that privacy is sacred and that he has a responsibility to defend both ideas.

"The public needs to decide whether these programs and policies are right or wrong," said Edward Joseph Snowden, the 29-year-old former National Security Agency (NSA) contractor who admitted on June 6 to one of the most significant thefts of highly classified secrets in U.S. history. The documents he turned over to the press revealed a massive program to compile U.S. telephone records into a database for antiterrorism and counterintelligence investigations. Another program, called Prism, has given the NSA access to records at major online providers like Google, Facebook and Microsoft to search information on foreign suspects with court approval. The secret program has been under way for seven years.

Snowden is "no different than anybody else," he claimed. "I'm just another guy who sits there day to day in the office," he said in an interview with the Guardian, which broke the story along with the Washington Post. But Snowden, who was working as an analyst for the government contractor Booz Allen, is not just another guy. He is something new. More than 1.4 million Americans now hold top-secret security clearances in the military and the shadow world of intelligence. Most do not contact reporters and activists over encrypted e-mail in hopes of publishing secrets as civil disobedience. Few are willing to give up their house, their $122,000-a-year job, their girlfriend or their freedom to expose systems that have been approved by Congress and two Presidents, under the close monitoring of the federal courts. Snowden is different, and that difference is changing everything.

A Brave New World

The U.S. National Security infrastructure was built to protect the nation against foreign enemies and the spies they recruit. Twenty-something homegrown computer geeks like Snowden, with utopian ideas of how the world should work, scramble those assumptions. Just as antiwar protesters of the Vietnam era argued that peace, not war, was the natural state of man, this new breed of radical technophiles believes that transparency and personal privacy are the foundations of a free society. Secrecy and surveillance, therefore, are gateways to tyranny. And in the face of tyranny, the leakers believe, rebellion is noble. "There is no justice in following unjust laws," wrote Aaron Swartz, a storied computer hacker and an early employee of Reddit, in a 2008 manifesto calling for the public release of private documents. "We need to take information, wherever it is stored, make our copies and share them with the world."

On the run in a Hong Kong hotel room, Snowden explained in a video interview the reasons for his actions, with pride and a hint of serenity, even as he described how he could be killed, secretly "rendered" by the CIA or kidnapped by Chinese mobsters for what he had done. He characterized the surveillance systems he exposed as "turnkey tyranny" and warned of what would happen if the safeguards now in place ever fell away. He hoped to force a public debate, to set the information free. "This is the truth. This is what is

happening," he said of the documents he had stolen and released. "You should decide whether we need to be doing this."

Three years earlier, a 22-year-old Army intelligence analyst stationed in Iraq named Bradley Manning offered a nearly identical defense for a similar massive breach of military and diplomatic secrets. "I want people to see the truth, because without information, you cannot make informed decisions as a public," Manning wrote to a hacking friend in 2010 after he had illegally sent hundreds of thousands of classified documents to the website WikiLeaks.

Like Snowden, Manning said his worst fear was not that his actions would change the world but that they wouldn't. Both young men grew up in the wake of the security crackdown that followed the Sept. 11, 2001 attacks. They had come of age online, in chat rooms and virtual communities where this new antiauthority, free-data ideology was hardening. They identified, at least in part, as libertarians, with Manning using the word to describe himself and Snowden sending checks to Ron Paul's presidential campaign. Neither appeared to believe he was betraying his country. "Information should be free," wrote Manning before his capture, later adding that he was not sure if he was a hacker, cracker, hacktivist, leaker or something else. "It belongs in the public domain."

"We Are Legion"

Manning's statement is a radical one, since it directly undermines the rule of law, something both men seemed to recognize. "When you are subverting the power of government, that's a fundamentally dangerous thing to democracy," Snowden said of his actions. And in official Washington, the broad consensus is that the impulse is dead wrong and likely to cause real harm. "What this young man has done, I can say with a fair amount of certainty, is going to cost someone their lives," said Georgia Republican Saxby Chambliss, who is vice chairman of the Senate Select Committee on Intelligence. Neither the Obama White House nor the leaders of either party are much concerned about the legality or the effectiveness of the sweeping data-collection programs; both sides, however, seemed quite keen to track down Snowden and bring him to justice. The public, according to a new TIME poll, echoed that impulse, with 53% of Americans saying Snowden should be prosecuted, compared with just 28% who say he should be sent on his way.

But among Snowden and Manning's age group, from 18 to 34, the numbers are much higher, with 43% saying Snowden should not be prosecuted. That hacktivist ethos is growing around the world, driven in large part by young hackers who are increasingly disrupting all manner of institutional power with online protest and Internet theft. "That's the most optimistic thing that is happening--the radicalization of the Internet-educated youth, people who are receiving their values from the Internet," said Julian Assange, the founder of WikiLeaks, in an April interview with Google executive chairman Eric Schmidt. "This is the political education of apolitical technical people. It is extraordinary."

The stories show up in newspapers and courtrooms on a daily basis. Just as Snowden flew to Hong Kong with his stolen cache, a 28-year-old hacker named Jeremy Hammond pleaded guilty in New York City on May 28 to stealing e-mails, credit-card information and documents from Stratfor Global Intelligence Service, a private consulting company. Hammond expressed little remorse for working with a hacking and activist collective known as Anonymous to break the law. "I did this because I believe people have a right to know what governments and corporations are doing behind closed doors," he wrote on a website after pleading guilty. "I did what I believe is right."

In recent years, Anonymous has targeted companies like MasterCard and trade groups like the Motion Picture Association of America for the alleged crime of opposing openness. They have staged protests against the rapid-transit system in the San Francisco Bay Area, when authorities shut down cellular service, and staged rallies around the world against Scientology, to protest the religion's aggressive protection of its secrets. In 2011, hackers claiming to be Anonymous stole personal details of 77 million Sony PlayStation accounts, shutting down the network for a month, in apparent protest of a prohibition the company had imposed on installing certain features on the devices' firmware.

Others have targeted academia and the law. Swartz, who committed suicide at the age of 26 in January while under federal indictment for hacking an academic computer, downloaded and publicly released millions of federal court documents from a U.S. court computer system in protest of a per-page fee for access. He was arrested for trying to download huge volumes of copyrighted academic articles from the costly JSTOR database at the Massachusetts Institute of Technology. "Those who have been locked out are not standing idly by," he had argued about the need to liberate information to the public domain.

These "free the files" protests are crimes under U.S. law, but in most cases they are not crimes of the nature the legal system was designed to prosecute. When they take the form of denial-of-service attacks, overwhelming and shutting down websites with bogus traffic, they resemble protests protected in some cases by the First Amendment. Others follow in the tradition of the country's most heralded technological revolutionaries. Facebook's Mark Zuckerberg hacked the Harvard databases of student IDs to create Facemash, the predecessor to his current multibillion-dollar site. As a teenager, Apple founder Steve Jobs sold boxes built by his friend Steve Wozniak to fool the phone company and make free long-distance calls. Microsoft's Bill Gates hacked the accounts of an early computer company to avoid having to pay to use it.

By the early 1990s, the hacktivists were organizing around larger goals, like ensuring online privacy for individuals. A hacker named Phil Zimmermann created a data-encryption program called PGP, which used a software technology that was classified as a "munition" under U.S. law and therefore banned for export. Zimmermann responded by publishing his code in a book, via MIT Press, since the export of printed matter is protected by the First Amendment. The movement that grew up around these efforts helped give birth to WikiLeaks. Today that same defiant spirit still dominates large swaths of the Internet, informing the actions of people like Snowden, Manning and Swartz. "It's a generation of kids who have been told again and again that behaviors that seem perfectly reasonable to them are criminal," says Lawrence Lessig, a Harvard law professor who was a mentor to Swartz.

Peter Ludlow, a philosophy professor at Northwestern University who has written extensively about cyberculture, says two disparate ideas have been linked in recent years. "There was always this kind of tech-hacker ethos, which was probably libertarian, which has collided with this antiauthoritarian political impulse," he said. "You put these two things together, and it's just like wildfire."

"We are legion," runs the catchphrase of Anonymous. "We do not forgive. We do not forget. Expect us." Now the government has to figure out how to respond.

Dawn of the Informer Age

In the days after the Snowden disclosures, a coalition of 86 groups--including online communities like 4chan, Reddit and BoingBoing--signed on to an open petition to Congress calling the NSA programs "unconstitutional surveillance." A petition filed with WhiteHouse.gov calling on Obama to pardon Snowden reached 60,000 names in three days. Sales of George Orwell's 64-year-old antitotalitarian novel 1984 have soared. The Progressive Change Campaign Committee, which usually raises money for liberal candidates, founded a legal-defense fund for Snowden. And a recent online video campaign--with Hollywood filmmaker Oliver Stone, actors such as Maggie Gyllenhaal and Peter Sarsgaard, and several liberal journalists--has been organizing a social-media campaign called "I am Bradley Manning," which argues Manning was nothing more than a whistle-blower who should be protected from prosecution.

Even the current corporate titans of Silicon Valley, who have long been libertarian in their politics, have not been far behind. Shortly after the Snowden leak named Google, Facebook and Microsoft as partners in the Prism program, the companies all asked the Justice Department for permission to disclose more fully their heretofore secret cooperation with the courts. The reason: they did not want to damage their brands, which have long embraced free experimentation and minimal regulation on the Internet. "Google has nothing to hide," the company's chief legal officer David Drummond announced in an open letter.

But what is accepted wisdom among the tech community is viewed with some skepticism with much of the American public. The TIME poll found that only 43% of the country thought the government should "cut back on programs that threaten privacy," while 20% said the government should be doing more, even if it invades privacy. On the question of whether they approved or disapproved of the current programs revealed by Snowden, the nation was basically split, with 48% approving and 44% disapproving.

The government, meanwhile, is likely to treat Snowden as if he was a Cold War spy seeking to undermine the country he still claims to serve. The Justice Department has launched an investigation into the disclosure of classified information, a prelude to a standard espionage prosecution. Even though charges may not be filed for weeks, it is likely that prosecutors will try to extradite Snowden to the U.S. for trial and seek a punishment of life in prison.

Perhaps the clearest summary of the federal response to this new online political activism can be found, appropriately enough, in a classified 2008 document from the U.S. Army Counterintelligence Center, which has been leaked and posted online by hacker activists. "Websites such as WikiLeaks.org have trust as their most important center of gravity protecting the anonymity and identity of the insider, leaker, or whistle blower," the document reads. The solution, concludes the Army, is to find, expose and punish those people who leak in an effort to "potentially damage or destroy this center of gravity and deter others considering similar actions."

Already, the government may have overinterpreted that guidance. Manning, after his arrest more than three years ago, was subjected to harsh incarceration conditions, including confinement to his cell 23 hours a day, that have raised the concerns of Amnesty International, a former U.N. human-rights investigator and even a former State Department spokesperson, Philip Crowley, who called the conditions "ridiculous and counterproductive and stupid." Crowley resigned over those comments, but a federal judge later ruled that Manning's final sentence would be reduced 112 days to compensate for harsh pretrial treatment.

Manning has already pleaded guilty to 10 counts of misusing classified information, with a maximum penalty of 20 years in prison. He is now undergoing a court-martial at Fort Meade, Maryland, the same military base where the NSA is headquartered, on additional charges of aiding the enemy and violating the Espionage Act, with the possibility of life in prison. "The more I read the cables, the more I came to the conclusion this was the type of information that should become public," he has testified in his own defense.

After the Manning leaks, the intelligence community, the State Department and the military tried to remake their procedures to ensure that another leak could not happen. New trip wires were added to detect massive downloading of classified information, monitor military workstations and better compartmentalize secret information. Clearly, more will have to be done. "There is a belief that the total revelation of information is in the public interest," said a White House official, describing the threat. The official noted that the coming changes to classified access in response to Snowden are likely to further limit information sharing, narrowing the potential of a key reform after 2001 meant to prevent further attacks.

"I think that there's a group of people, younger people who are not fighting the war, who are libertarians mostly, who feel like the government is the problem," says Senator Lindsey Graham, the South Carolina Republican on the Armed Services Committee who helped write the laws that govern the NSA surveillance programs. Graham says he wants more internal efforts in the intelligence community to detect such people before they go public and to punish the leakers severely. "It's imperative that we catch him," Graham said of Snowden. "I don't care what we need to do. We need to bring this guy to justice for deterrence sake."

But others who monitor the intelligence world say it will not be so easy. Snowden wasn't a government official; he was a private contractor, the kind of hired help the U.S. intelligence system has come to rely on by the thousands since 9/11. And the punishment of Manning did not dissuade Snowden, after all. If anything, it cleared the path to future celebrity and martyrdom for other, like-minded activists. "It's going to be a challenge to the intelligence community to figure out how to defend against this," says Senator Chambliss. "I don't know that you always can."

In the meantime, the threat of more leaks is likely to grow as young people come of age in the defiant culture of the Internet and new, principled martyrs like Snowden seize the popular imagination. "These backlashes usually do provoke political mobilization and a deepening of commitments," says Gabriella Coleman, a professor at McGill University in Montreal, who is finishing a book on Anonymous. "I kind of feel we are at the dawn of it."

The original version of this story incorrectly identified Aaron Swartz as a co-founder of the website Reddit. In fact, he joined the company about 6 months after its inception.