Edward Snowden, The Dark Prophet

Time, December 11, 2013, "Person of the Year Runner-Up"

He pulled off the year's most spectacular heist. Exiled from his country, the 30-year-old computer whiz has become the doomsayer of the information age

By Michael Scherer


Illustration by Jason Seiler for TIME

To avoid surveillance, the first four Americans to visit Edward Snowden in Moscow carried no cell phones or laptops. They flew coach on Delta from Washington with tickets paid for by Dutch computer hackers. After checking into a preselected hotel not far from Red Square, they waited for a van to pick them up for dinner.

None could retrace the ride that followed, driven by anonymous Russian security men, nor could any place the side door of the building where the trip ended. They passed through two cavernous ballrooms, the second with a painted ceiling like the Sistine Chapel, and emerged into a smaller space with salmon-colored walls and oil paintings in golden frames—like Alice in Wonderland, remembers one of the group. There at the bottom of the rabbit hole, in rimless glasses, a black suit and blue shirt with two open buttons at the collar, stood the 30-year-old computer whiz who had just committed the most spectacular heist in the history of spycraft.

By all accounts, Snowden was delighted to see his countrymen, though over the next six hours he did not partake of the wine. At one point, Ray McGovern, a former CIA analyst, recited from memory in Russian an Alexander Pushkin poem, "The Prisoner," which he had learned back in

his days spying on the Soviet Union. “We have nothing to lose except everything, so let us go ahead,” said Jesselyn Radack, a former Justice Department attorney, quoting Albert Camus’s warning at the dawn of the nuclear age. Another attendee, the whistle-blowing FBI agent Coleen Rowley, compared Snowden to Benjamin Franklin, who as postmaster general in 1773 helped leak letters from American officials who were secretly collaborating with British authorities.

Even Snowden’s Russian lawyer, Anatoly Kucherena, raised his glass for a toast. Coming from a man with close ties to the Kremlin and a knack for misleading the press, Kucherena’s words captured the surreal nature of Snowden’s Moscow exile. “Ed, I am going to give you the biggest gift that I can probably give,” he told Snowden through an interpreter. “I’m writing a novel about you.”

The gathering had been called to deliver an award, given by four dissident veterans of the U.S. national-security apparatus to one of their own. But for Snowden it was something more, a chance to reaffirm to the world the purpose of his actions, for which he has been charged in absentia with theft and violations of the Espionage Act. Since escaping his country in late May with tens of thousands of its most secret documents—“one of everything,” jokes one person with access to the stash—Snowden has chosen to lie low. No Twitter account. No television interviews. No direct contacts with U.S. authorities. He held his tongue as Kucherena boasted to the press about Snowden’s new Internet job in Moscow, his new Russian girlfriend and his dire money troubles. Most of that is fiction, like the novel, according to several people who communicate regularly with Snowden.

But he has nonetheless begun to figure out a life for himself in Russia, where he has been granted asylum for at least one year. He is learning Russian, recently read Fyodor Dostoyevsky’s *Crime and Punishment* and spent weeks living with his WikiLeaks protector, Sarah Harrison, who has since flown to Berlin, fearing that she could face criminal charges if she returns to her native Britain. Most important, he has been able to spend time on the Internet, his lifelong home, where he has watched through encrypted and anonymized connections as his leaks roil the world—diplomatic crises, congressional reform efforts, new federal lawsuits, financial damage to U.S. technology companies and an as yet uncertain harm to U.S. national interests, including documented changes in the way terrorists communicate online. “This increases the probability that a terrorist attack will get through,” says General Keith Alexander, the director of the National Security Agency (NSA). “I think it’s absolutely wrong.”

For Snowden, those impacts are but a means to a different end. He didn’t give up his freedom to tip off German Chancellor Angela Merkel about the American snoops on her cell phone or to detail the ways the NSA electronically records jihadi porn-watching habits. He wanted to issue a warning to the world, and he believed that revealing the classified information at his fingertips was the way to do it. His gambit has so far proved more successful than he reasonably could have hoped—he is alive, not in prison, and six months on, his documents still make headlines daily—but his work is not done, and his fate is far from certain. So in early October, he invited to Moscow some supporters who wanted to give him an award.


EPA

Snowden received the Sam Adams Associates for Integrity in Intelligence award in Moscow in October.

After the toasts, some photographs and a brief ceremony, Snowden sat back down at the table, spread with a Russian buffet, to describe once again the dystopian landscape he believes is unfolding inside the classified computer networks on which he worked as a contractor. Here was a place that collected enormous amounts of information on regular citizens as a precaution, a place where U.S. law and policy did not recognize the right to privacy of foreigners operating outside the country, a place where he believed the basic freedoms of modern democratic states—"to speak and to think and to live and be creative, to have relationships and to associate freely"—were under threat.

"There is a far cry between legal programs, legitimate spying, legitimate law enforcement—where it is targeted, it's based on reasonable suspicion, individualized suspicion and warranted action—and the sort of dragnet mass surveillance that puts entire populations under a sort of an eye and sees everything, even when it is not needed," Snowden told his colleagues. "This is about a trend in the relationship between the governing and governed in America."

That is the thing that led him to break the law, the notion that mass surveillance undermines the foundations of private citizenship. In a way, it is the defining critique of the information age, in which data is increasingly the currency of power. The idea did not originate with Snowden, but no one has done more to advance it. "The effect has been transformative," argues Julian Assange, the founder of WikiLeaks, who has been helping Snowden from the confines of the Ecuadorean embassy in London. "We have shifted from a small group of experts understanding what was going on to broad public awareness of the reality of NSA mass surveillance." If Facebook's Mark Zuckerberg is the sunny pied piper of the new sharing economy, Snowden has become its doomsayer.

The Information Grid

When electronic surveillance began, with the invention of the telegraph and radio, the only way to record an intercept was with ink and paper. Now there are technologies that allow for the wholesale copying, sorting and storage of billions of records a day—everything that passes through a fiber-optic cable, for instance, or gets beamed through the airwaves. By itself, this is a revolutionary development. But its real power comes from the way regular people have changed

their behavior. In the 19th century, humans rarely produced electronic signals. Now almost every part of daily existence can cast off bits and bytes.

The cell phone in your pocket records your movements and stores that information with your service carrier. The e-mail, chat and text messages you create map your social relations and record your thoughts. Credit-card purchases show spending habits and tastes. Mass-transit databases note when you board subways and buses with fare cards. The search terms you enter into your laptop—preserved by Google in ways that can be used to identify your computer for a standard period of nine months—may tell more about your deepest desires than anything you would ever admit to a friend or lover.

Then there are the emerging technologies that will soon add even more information to the grid: The wearable-computing devices that monitor your pulse. The networked surveillance cameras rigged with facial-recognition software. The smart meters that record what time of night you turn out the lights. Retail companies like Nordstrom and Apple have debuted technologies that use your cell phones to track how long you linger before any single display. The possibilities are dizzying, and your information funds the whole enterprise. "Surveillance is the business model of the Internet," explains Bruce Schneier, a security technologist who has access to some of the documents Snowden provided.

Snowden's theft revealed a massive, secret U.S. national-security state—$52.6 billion a year, with more than 30,000 employees at the NSA alone—struggling to come to grips with this new surveillance potential in the wake of the 2001 terrorist attacks. Electronic intelligence historically focused on foreign governments and their public officials, but the hijackers who took down the World Trade Center were private individuals, born abroad and living in the homeland. So as the rubble still smoldered, the great arrays set up by the NSA turned inward and shifted focus. The subjects of collection grew to include patterns within entire populations and historical data that could literally retrace the steps of individuals years before they became suspects. The challenge, explained one NSA document made public by Snowden, was to "master global networks and handle previously unimagined volumes of raw data for both passive and active collection."

So new databases were built, and ground was broken on a massive classified data center in the Utah desert that will need as much as 1.7 million gal. (6.4 million L) of water a day just to keep the computer servers cool. And the data was collected. Since 2006 the U.S. government has gathered and stored transaction records of phone calls made in America. For a time, the government sucked up similar metadata on Internet traffic as well. Cellular location data, mostly from foreign-owned phones, has also been collected, with some 5 billion records a day absorbed by databases that can later be used to reconstruct a person's movements or find out who joins a meeting behind closed doors.

One NSA document released by Snowden estimated that 99% of the world's Internet bandwidth in 2002 and 33% of the world's phone calls in 2003 passed through the U.S., an accident of history that proved a gold mine to sift through, with or without the cooperation of American companies. The agency hacked overseas cables and satellites and surreptitiously sucked information transiting among foreign cloud servers of U.S. technology companies like Google and Yahoo. It harvested and stored hundreds of millions of contact lists from personal e-mail and

instant-messaging accounts on services like Yahoo and Facebook. A program called Dishfire sucked up years' worth of text messages from around the world, and a database by the name of Tracfin captured credit-card transactions. "High performance computing systems must extract meaning from huge data sets and negate data encryption and computer access controls," reads a 2007 classified NSA mission statement released by Snowden. "Fortunately, information management and mining is central to the Internet age."

The NSA is not the only one playing the game. It just does it better, on a grander scale, than anyone else, at least so far. Russia and China have similar surveillance infrastructures, say current and former U.S. officials, and petty dictatorships the world over have been buying their technology on the open market. When rebels overthrew Libyan strongman Muammar Gaddafi in 2011, they found a device from the French company Amesys that allowed the dictator to gather up and search in bulk the Internet traffic generated by his people. No Libyan activist had been safe to send an unencrypted e-mail or post a Facebook comment. The company's sales pitch, later leaked to WikiLeaks, began with a slide that read, "From lawful to massive interception."

Privacy Protections

With all this information now public, the important questions are easy to spot: What should distinguish democratic governments from totalitarian ones in an era of mass surveillance? Are privacy protections a human right or just a convenience of nationality? Can the massive U.S. national-security apparatus be trusted to make the right choices in secret when the next crisis comes? Even President Obama encourages the conversation as he continues to seek Snowden's imprisonment. "I think it's healthy for our democracy," he said just weeks before the White House refused to confirm or deny its role in rerouting the plane carrying Bolivian President Evo Morales after a false rumor that Snowden was on board.

In an interview with Time conducted via e-mail in early December, Snowden explained his answers to those big questions, even as he allowed for the fact that the U.S. public he sees himself serving may not ultimately agree. The privacy of regular citizens, he believes, is a universal right, and the dangers of mass surveillance litter the dark corners of the 20th century. "The NSA is surely not the Stasi," he argued, in reference to the notorious East German security service, "but we should always remember that the danger to societies from security services is not that they will spontaneously decide to embrace mustache twirling and jackboots to bear us bodily into dark places, but that the slowly shifting foundation of policy will make it such that mustaches and jackboots are discovered to prove an operational advantage toward a necessary purpose."

Snowden's hope, he continued, is that the disclosure will force five distinct civic bodies—the public, the technologist community, the U.S. courts, Congress and the Executive Branch—to reconsider the path ahead. "The President," Snowden wrote, "could plausibly use the mandate of public knowledge to both reform these programs to reasonable standards and direct the NSA to focus its tremendous power toward developing new global technical standards that enforce robust end-to-end security, ensuring that not only are we not improperly surveilling individuals but that other governments aren't either."

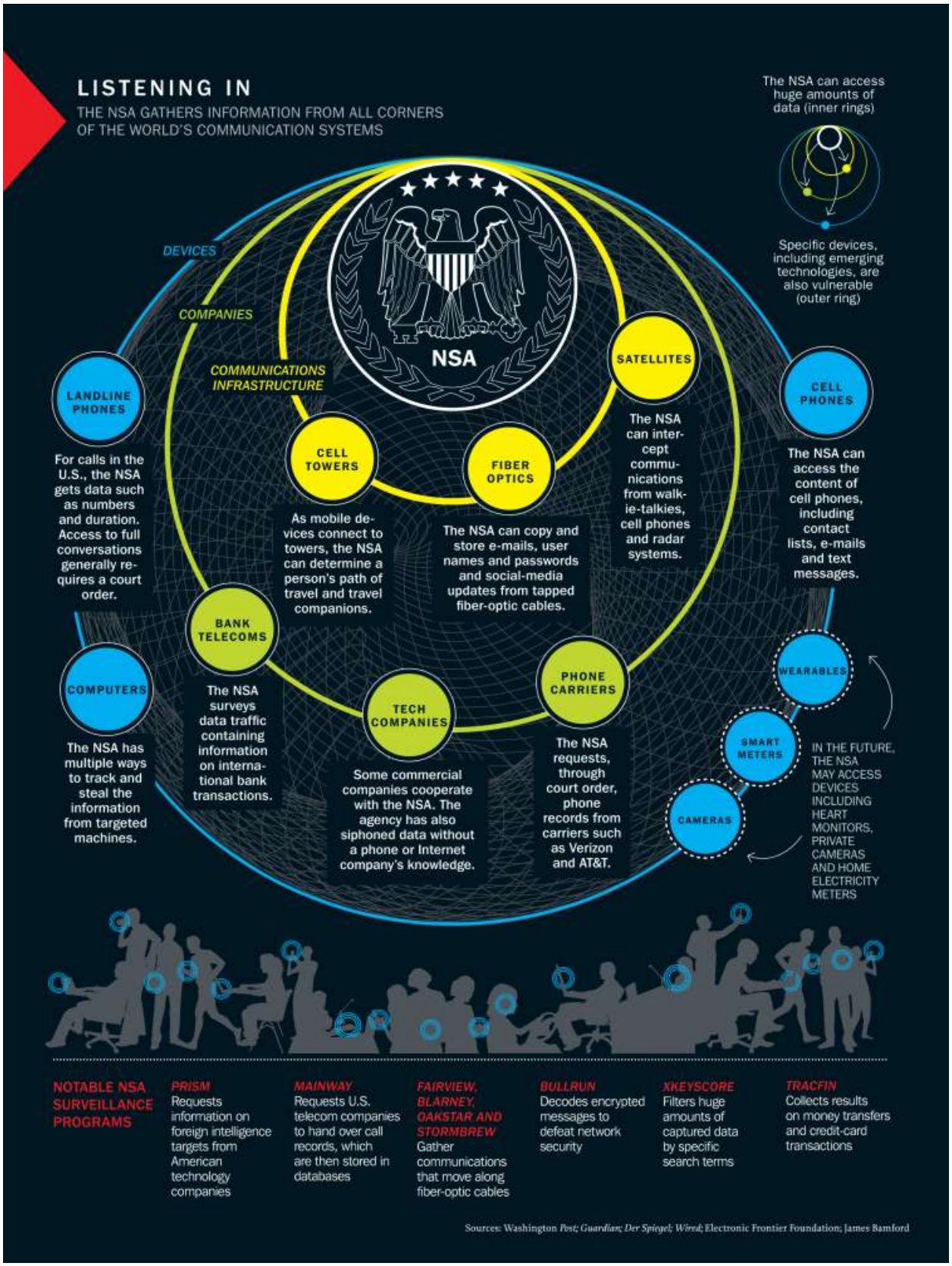
As for the technologists like him, it is important that they know as well what is being done, so they can invent new ways to protect citizens. “There is a technical solution to every political problem,” Snowden argued. One of the NSA programs he revealed, called Bullrun, described a $250 million annual effort to engage with “the U.S. and foreign IT industries to covertly influence and/or overtly leverage their commercial products’ designs,” providing the spies a back door to encrypted communications. Though the law-enforcement purpose of such an effort is clear, as terrorists and foreign powers experiment with encryption, Snowden believes private citizens also have a right to create unbreakable encryption software. “In general, if you agree with the First Amendment principles, you agree with encryption. It’s just code,” he wrote in an e-mail to Time. “Arguing against encryption would be analogous to arguing against hidden meanings in paintings or poetry.”

America In the Dark

The NSA, for its part, has always prided itself on being different from the intelligence services of authoritarian regimes, and it has long collected far less information on Americans than it could. The programs Snowden revealed in U.S. surveillance agencies, at least since the 1970s, are subject to a strict, regularly audited system of checks and balances and a complex set of rules that restrict the circumstances under which the data gathered on Americans can be reviewed. As a general rule, a court order is still expected to review the content of American phone calls and e-mail messages. Unclassified talking points sent home with NSA employees for Thanksgiving put it this way: “The NSA performs its mission the right way—lawful, compliant and in a way that protects civil liberties and privacy.” Indeed, none of the Snowden disclosures published to date have revealed any ongoing programs that clearly violate current law, at least in a way that any court has so far identified. Parts of all three branches of government had been briefed and had given their approval.

But the court rulings and briefing books that undergird the surveillance programs have long been so highly classified and technically complex that they remained opaque to the public. Snowden believed that the standard for review needed to be different, with transparent public debate and open court proceedings. In the tradition of other national-security whistle-blowers, who have played a role in the messy American system of checks and balances by leaking the Pentagon Papers and the details of President George W. Bush’s warrantless wiretapping program, Snowden decided he had an individual obligation to defy his government and his own contractual obligations. “What we recoil most strongly against is not that such surveillance can theoretically occur,” he wrote to Time, “but that it was done without a majority of society even being aware it was possible.”

At the time Snowden went public, the American people had not just been kept in the dark; they had actively been misled about the actions of their government. The provision of the 2001 Patriot Act that allowed for the collection of American phone records, for instance, was publicly described as analogous to a grand jury subpoena by the Department of Justice, suggesting individual secret warrants. But secret interpretations told a different story. “Tell me if you’ve ever seen a grand jury subpoena that allowed the government on an ongoing basis to collect the records of millions of ordinary Americans,” said Oregon Senator Ron Wyden, a longtime critic of the programs, in a recent speech



| TIME Graphic by Heather Jones

In a 2012 speech, NSA director Alexander said, “We don’t hold data on U.S. citizens,” a statement he apparently justified with an unusual definition of the word hold. Months later, National Intelligence Director James Clapper told Congress in an open session that the NSA did not “collect” any type of data on millions of Americans. After the Snowden documents were leaked, Clapper apologized for his “clearly erroneous” answer, saying he was only giving the “least untruthful” response possible in an unclassified setting. “When someone says ‘collection’ to me, that has a specific meaning, which may have a different meaning to him,” Clapper said.

Intelligence officials have now been forced to join the public debate, and Obama has authorized the declassification of thousands of pages of documents. Nonetheless, current and former government officials say the way Snowden went about leaking his documents and the documents he selected will cause clear harm to his country’s legitimate interests. “We have seen, in response to the Snowden leaks, al-Qaeda and affiliated groups seeking to change their tactics,” warned Matthew Olson, director of the National Counterterrorism Center, in July. Snowden has maintained that he did not download information that would put other intelligence officials in danger or give up sources and specific methods to foreign rivals of the U.S. But his disclosures were also not limited to revealing the mass surveillance of otherwise innocent civilian populations.


Kirill Kudryavtsev / AFP / Getty Images

In late June, Snowden was booked in window seat 17A of this Aeroflot plane flying from Moscow to Havana, but he never boarded.

While in Hong Kong, Snowden gave an interview and documents to the South China Morning Post describing NSA spying on Chinese universities, a disclosure that frustrated American attempts to embarrass China into reducing its industrial-espionage efforts against U.S. firms. A story that showed up in Der Spiegel, using Snowden documents, showed how British spies working with the U.S. used fake LinkedIn accounts to install malware on the computers of foreign telecom providers. Other stories have given details on NSA spying operations on traditional surveillance targets like diplomatic delegations at international summits. And many of the most controversial disclosures in the Snowden documents concern not mass surveillance but the targeting of foreign leaders. “They’re being put out in a way that does the maximum damage to NSA and our nation,” says Alexander. “And it’s hurting our industry.”

American technology and telecommunications companies, some of which have long histories of cooperating with the NSA, have also suffered as a result, and they are scrambling to increase encryption of their systems and assure foreign customers of their commitment to privacy. A December paper by eight U.S. technology giants, including Apple, Facebook and Google, called on the U.S. government to end to "bulk data collection of Internet communications" and "limit surveillance to specific, known users for lawful purposes." In India, government officials may soon be barred from using e-mail with servers located in the U.S., and recent estimates say the risk to American firms in the emerging marketplace for cloud computing could reach $180 billion. In a recent earnings call, Robert Lloyd—president of development for Cisco Systems, a provider of Internet hardware—said the revelations were already affecting overseas sales. "It's certainly causing people to stop and then rethink decisions, and that is, I think, reflected in our results," he said.

From Russia, Snowden does not defend every story that has been written, but he says he tried to design his actions to ensure that he was not the ultimate arbiter of what should and should not become public. "There have of course been some stories where my calculation of what is not public interest differs from that of reporters, but it is for this precise reason that publication decisions were entrusted to journalists and their editors," he told Time. "I recognize I have clear biases influencing my judgment."

That question of judgment is at the heart of the issues Snowden has raised. Polls still show Americans largely conflicted about the programs that have been revealed. Since the disclosures, a majority of Americans say they believe their privacy rights have been violated. But polls also show continued willingness to give up limited amounts of privacy as part of efforts to combat terrorism.

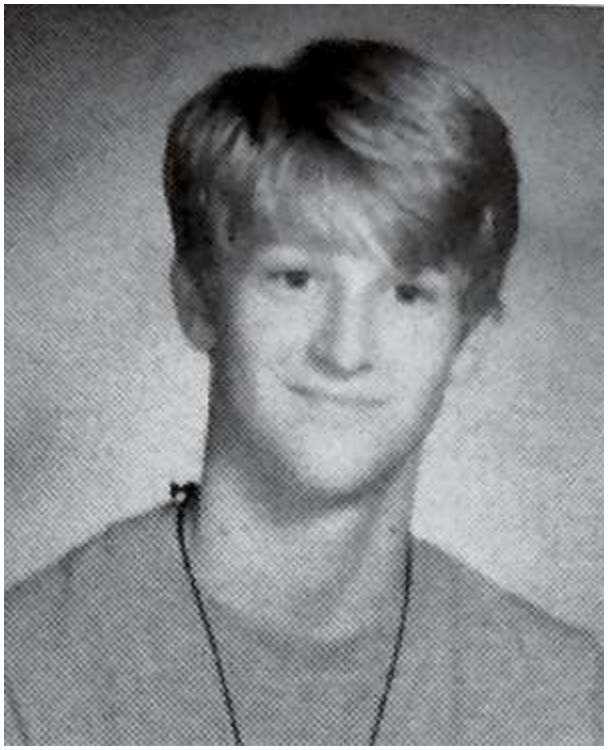
The most striking numbers show a generation gap in the way people think about Snowden. Just 35% of Americans ages 18 to 30 say Snowden should be charged with a crime, compared with 57% of those 30 and older, according to a November poll by the Washington Post and ABC News. And 56% of young adults say he did the "right thing," compared with 32% of their elders. Younger people, who are moving away from Facebook and embracing technologies like Snapchat, which destroys messages after a few seconds, have also been shown to spend far more time than their elders tightening privacy settings on phones and apps. "Snowden is an effect, not a cause," says General Michael Hayden, a recently retired director of both the NSA and CIA. "This new generation has a different take on where the appropriate line is."

The shifts could have far greater implications than just what apps people choose for their smartphones. Historically, the Fourth Amendment of the Constitution, which offers no protections for noncitizens outside the country, has been the source of privacy protections under U.S. law. But the rhetoric now coming from European governments and even senior officials of the Obama Administration points to broader, as yet undefined rights, which several countries are now seeking to codify in international law at the U.N. "We must use the unprecedented power that technology affords us responsibly, while respecting the values of privacy, government transparency and accountability that all people share," said National Security Adviser Susan Rice in a December speech.

Growing Up Online

Snowden dropped out of high school and got a GED. The fourth American to attend Snowden's October awards ceremony was Thomas Drake, who, like Snowden, was a veteran of the NSA and a former contractor for Booz Allen Hamilton. For years after the Sept. 11 attacks, Drake sounded alarm bells with Congress and the military about the NSA's behavior, eventually deciding to give unclassified information about certain programs to a reporter for the Baltimore Sun. For this, he was charged under the Espionage Act on flimsy charges that fell apart in court but still caused Drake years of hardship. When the Americans walked in for dinner in Moscow, - McGovern remembers that Snowden looked past him and focused on Drake, whom Snowden had never met before but had long regarded as a role model. "I was an inspiration to him," Drake acknowledges. "He represents, for me, the future."

Like Snowden, Drake grew up online, living his life inside the nascent Internet, finding friendships and forming an identity. His first computer, in the 1980s, was an Atari 8-bit. "I lived a double life, the virtual life in this digital space, in this transnational space," says Drake, who is now 56. "It was unbelievable, this culture of sharing information."



Arundel Schools / Splash News / Corbis

For Snowden, a high school dropout with a GED who grew up just miles from the NSA's headquarters in Maryland, the Internet was also always a source of identity. His father, a Coast Guard officer, and his mother, a clerk in federal court, separated when he was young. As a teen, he spent years playing games online. As a young CIA employee in Switzerland, he vented and

socialized regularly on anonymous chat boards. In this virtual space, national borders mattered less, and electronic privacy mattered more. By the time he had risen to become a senior technical consultant for the CIA, working as a Dell contractor, those values remained. “The one thing you resisted was this authoritarian power that wanted to own you,” says Drake, who will quote Star Trek and Tron to explain his values. “I was with the user.”

At some point in the coming months or years, Snowden’s fate will be decided. It is not clear if his asylum in Russia will be renewed. He continues to receive financial support from abroad, and a team of lawyers around the world is working on his behalf, pursuing other asylum applications and waiting on offers of negotiation from the U.S. authorities. Though the Department of Justice has promised not to apply the death penalty, no other offers of leniency have been forthcoming.

As the dinner wound down, Harrison, Snowden’s WikiLeaks adviser, explained to the group why she had put her life in legal jeopardy to help Snowden. “There needs to be another narrative,” she said in reference to Chelsea Manning, the U.S. Army private formerly known as Bradley, who leaked massive amounts of documents and was sentenced to 35 years in prison. “There needs to be a happy ending. People need to see that you can do this and be safe.”

Snowden, a libertarian activist who gave up his freedom only to live at the whim of an authoritarian state, has not fully succeeded in that regard. But he will not be the last of his kind, either. Both Assange and Laura Poitras, one of the first journalists Snowden contacted, say his efforts have already emboldened other leakers. “What Snowden did was really empowering,” says Poitras. “I mean, think of all the people who have security clearance. There are hundreds of thousands, millions of them. They see that this is really a historic moment, and they are starting to question their belief in the job they were asked to do.”

It is an odd corollary to this new era of mass surveillance: the same technologies that give states vast new powers increase the ability of individuals on the inside to resist. Those dynamics are fixed, a code that underpins the world we now inhabit. That is what Snowden ultimately realized and exploited, a matter of simple physics. His example is the most consequential and dramatic, but it is unlikely to be the last.

—with reporting by Simon Shuster/Berlin