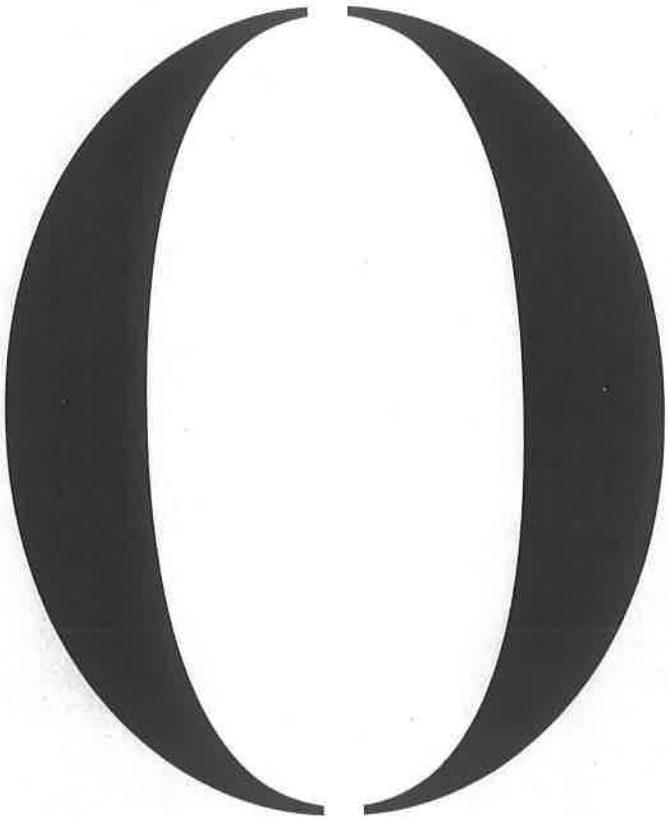


ON JUNE 6, 2013, *Washington Post* reporters called the communications departments of Apple, Facebook, Google, Yahoo, and other Internet companies. The day before, a report in the British newspaper *The Guardian* had shocked Americans with evidence that the telecommunications giant Verizon had voluntarily handed a database of every call made on its network to the National Security Agency. The piece was by reporter Glenn Greenwald, and the information came from Edward Snowden, a 29-year-old IT consultant who had left the US with hundreds of thousands of documents detailing the NSA's secret procedures. ¶ Greenwald was the first but not the only journalist that Snowden reached out to. The *Post*'s Barton Gellman had also connected with him. Now, collaborating with documentary filmmaker and Snowden confidante Laura Poitras, he was going to extend the story to Silicon Valley. Gellman wanted to be the first to expose a top-secret NSA program called Prism. Snowden's files indicated that some of the biggest companies on the web had granted the NSA and FBI direct access to their servers, giving the agencies the ability to grab a person's audio, video, photos, emails, and documents. The government urged Gellman not to identify the firms involved, but Gellman thought it was important. "Naming those companies is what would make it real to Americans," he says. Now a team of *Post* reporters was reaching out to those companies for comment.

It would be the start of a chain reaction that threatened the foundations of the industry. The subject would dominate headlines for months and become the prime topic of conversation in tech circles. For years, the tech companies' key policy issue had been negotiating the delicate balance between maintaining customers' privacy and providing them benefits based on their personal data. It was new and controversial territory, sometimes eclipsing the substance of current law, but over time the companies had achieved a rough equilibrium that allowed them to push forward. The instant those phone calls from reporters came in, that balance was destabilized, as the tech world found itself ensnared in a fight far bigger than the ones involving oversharing on Facebook or ads on Gmail. Over the coming months, they would find themselves at war with their own government, in a fight for the very future of the Internet.

But first they had to figure out what to tell the *Post*. "We had 90 minutes to respond," says Facebook's head of security, Joe Sullivan. No one at the company had ever heard of a program called Prism. And the most damning implication—that Facebook and the other companies granted the NSA direct access to their servers in order to suck up vast quantities of information—seemed outright wrong. CEO Mark Zuckerberg was taken aback by the charge and asked his executives whether it was true. Their answer: no.

Similar panicked conversations were taking place at Google, Apple, and Microsoft. "We asked around: Are there any surreptitious ways of getting information?" says Kent Walker, Google's general counsel. "No."

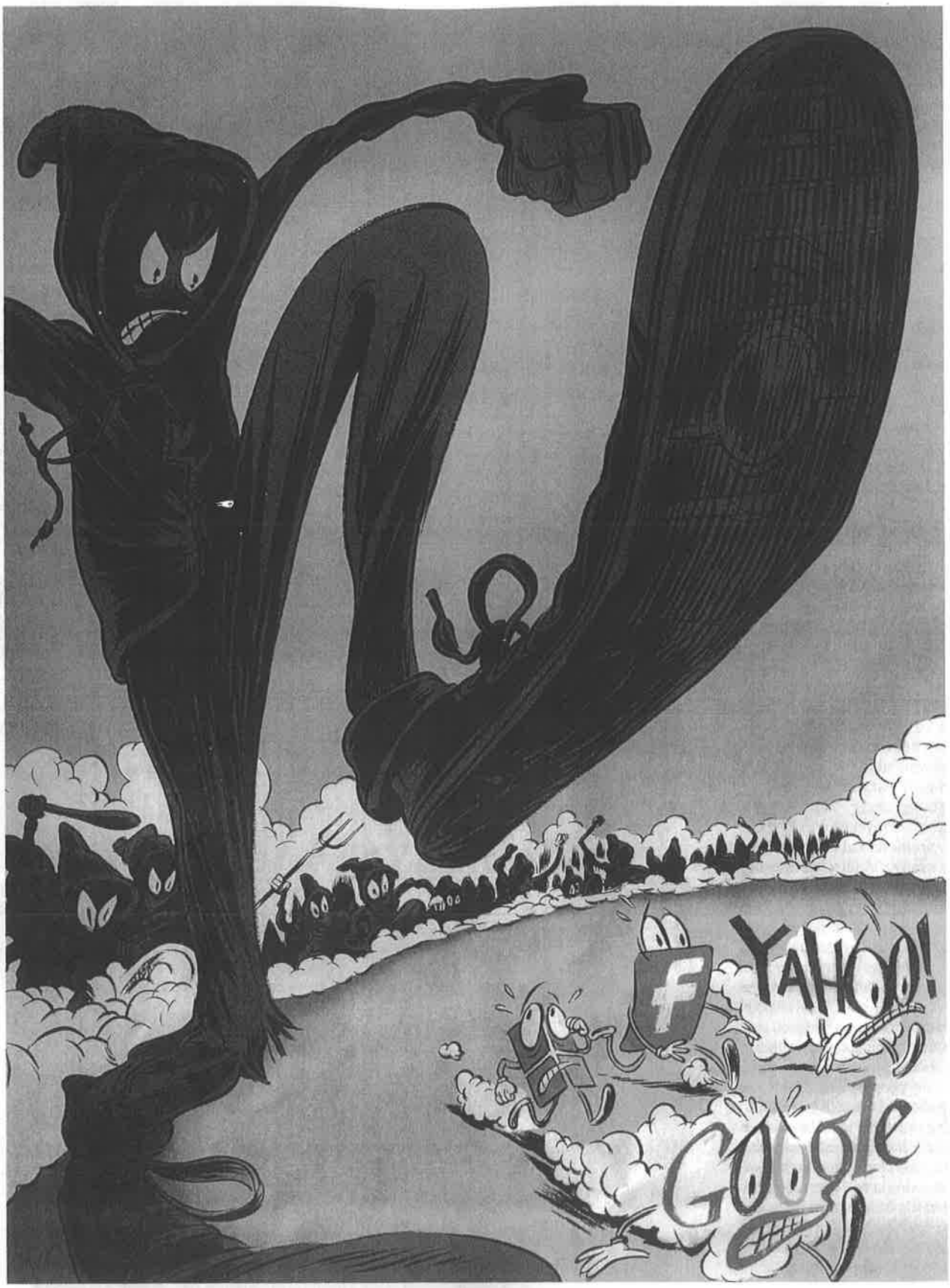
Nevertheless, the *Post* published its report that day describing the Prism program. (*The Guardian* ran a similar story about an hour later.) The piece included several images leaked from a 41-slide NSA PowerPoint, including one that listed the tech companies that participated in the program and the dates they ostensibly began fully cooperating. Microsoft came first, in September 2007, followed the next year by Yahoo. Google and Facebook were added in 2009. Most recent was Apple, in October 2012. The slide used each company's corporate logo. It was like a sales force boasting a series of trophy contracts. Just a day earlier, the public had learned that Verizon and probably other telephone companies had turned over all their call records to the government. Now, it seemed, the same thing was happening with email, search history, even Instagram pictures.

The tech companies quickly issued denials that they had granted the US government direct access to their customers' data. But that stance was complicated by the fact that they *did* participate—often unwillingly—in a government program that required them to share data when a secret court ordered them to do so. Google and its counterparts couldn't talk about all the details, in part because they were legally barred from full disclosure and in part because they didn't *know* all the details about how the program actually worked. And so their responses were seen less as full-throated denials than mealy-mouthed contrivances.

They hardly had the time to figure out how to frame their responses to Gellman's account before President Obama weighed in. While implicitly confirming the program (and condemning the leak), he said, "With respect to the Internet and emails, this does not apply to US citizens and does not apply to people living in the United States." This may have soothed some members of the public, but it was no help to the tech industry. The majority of Apple, Facebook, Microsoft, and Yahoo customers are not citizens of the US. Now those customers, as well as foreign regulatory agencies like those in the European Union, were being led to believe that using US-based services meant giving their data directly to the NSA.

The hard-earned trust that the tech giants had spent years building was in danger of evaporating—and they seemed powerless to do anything about it. Legally gagged, they weren't free to provide the full context of their cooperation or resistance. Even the most emphatic denial—a blog post by Google CEO Larry Page and chief legal officer David Drummond headlined, "What the ..."—did not quell suspicions. How could it, when an NSA slide indicated that anyone's personal information was just one click away? When Drummond took questions on the *Guard-*

STEVEN LEVY (@stevenlevy) *is a senior staff writer at* WIRED *and the author of* Crypto.



"Every time we spoke **it seemed to make matters worse,"** one tech executive says. "We just were not believed."

ZOHAR LAZAR

ian website later in the month, his interlocutors were hostile:

"Isn't this whole show not just a face-saving exercise ... after you have been found to be in cahoots with the NSA?"

"How can we tell if Google is lying to us?"

"We lost a decade-long trust in you, Google."

"I will cease using Google mail."

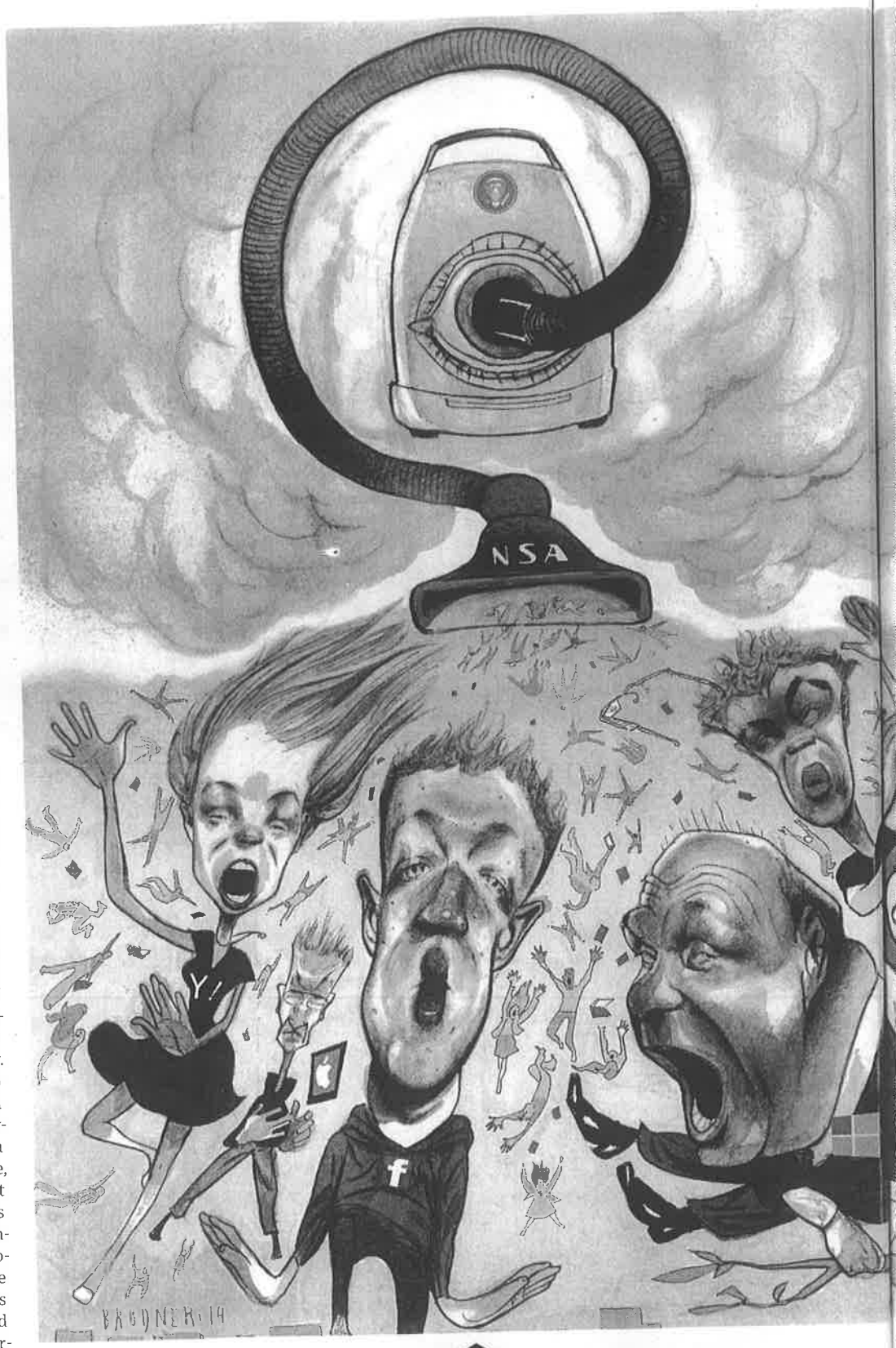
The others under siege took note. "Every time we spoke it seemed to make matters worse," an executive at one company says. "We just were not believed."

"The fact is, the government can't put the genie back in the bottle," says Facebook's global communications head, Michael Buckley. "We can put out any statement or statistics, but in the wake of what feels like weekly disclosures of other government activity, the question is, will anyone believe us?"

At an appearance at a tech conference last September, Facebook's Zuckerberg expressed his disgust. "The government blew it," he said. But the consequences of the government's actions—and the spectacular leak that informed the world about it—was now plopped into the problem set of Zuckerberg, Page, Tim Cook, Marissa Mayer, Steve Ballmer, and anyone else who worked for or invested in a company that held customer data on its servers.

Not just revenue was at stake. So were ideals that have sustained the tech world since the Internet exploded from a Department of Defense project into an interconnected global web that spurred promises of a new era of comity. The Snowden leaks called into question the Internet's role as a symbol of free speech and empowerment. If the net were seen as a means of widespread surveillance, the resulting paranoia might affect the way people used it. Nations outraged at US intelligence-gathering practices used the disclosures to justify a push to require data generated in their countries to remain there, where it could not easily be hoovered by American spies. Implementing such a scheme could balkanize the web, destroying its open essence and dramatically raising the cost of doing business.

Silicon Valley was reeling, collateral damage in the war on terror. And it was only going to get worse.



"At first we were in an arms race with sophisticated criminals," Google's head of security says. **"Now we're in an arms race with the best nation-state actors."** Primarily, the US government.

STEVE BRODNER

WHILE TECH COMPANIES didn't know the name Prism before June, they came to understand that it refers to a program several years old, in which they turn over specified data to the government, often without formal warrants, for national security purposes. The program's legal justification derives from a series of laws, renewals, and extensions. The Foreign Intelligence Security Act of 1978, widely referred to as FISA, created a secret court that blesses information requests. The FISA Amendments Act of 2008 carved out a new section of the law, 702, which gave legal cover to the warrantless surveillance programs operated in total secrecy under President Bush; queries are often called 702s. The NSA cites the FISA Amendments Act as the specific legal basis for Prism. More covert surveillance practices (outside of Prism) are justified under Reagan-era Executive Order 12333, which authorized the NSA to collect pretty much any data from outside the US that concerns foreign persons.

In a sense, Prism is a child of the Patriot Act, which set a post-9/11 tone for the sacrifice of some civil liberties in service of national security. "It was passed in the middle of a huge, understandable fear," says US senator Ron Wyden (D-Oregon), who voted for it and is a member of the Senate Intelligence Committee. "I felt it had a time stamp on it. Nobody reading it would be inclined to think of bulk collection of data on millions and millions of Americans."

Some companies seemed perfectly comfortable turning over information about their customer bases to the NSA. Verizon has never denied passing along its key billing information, including the number and duration of every call made by each of its millions of customers. In a way, this isn't surprising. Telephone companies don't sell themselves on trust, and customers have few expectations of their relationship with those quasi-monopolistic behemoths. Instead of catering to consumers, telcos seem to prioritize winning favor with the government that regulates them.

Technology companies are another matter. It's almost a cliché when tech CEOs claim that without the trust of their users, they would have no business. They depend on customers' willingness to share information. In exchange, those customers receive more and better services, and expect that the companies will keep their personal data private and secure and will be transparent about any exceptions. Users had no reason to think their information would be handed over to the government without a warrant.

At least one company challenged those requests as unconstitutional. Yahoo waged a secret battle in the FISA court to resist turning over user data. But it was for naught. An August 22, 2008, order determined that the government's interest in national security, along with safeguards in the program, outweighed privacy concerns in a manner consistent with the law. A subsequent appeal went nowhere. Yahoo's unsuccessful challenge set a marker for those who might resist in the future: The FISA request program was legal, and any company that failed to cooperate would risk the contempt charges specified in the law.

The requests might have offended some of the large tech companies but weren't logistically challenging. None say they were forced to make significant infrastructure changes as a result. Generally they would divert requested data to special equipment owned by the government. In some cases they even hosted the equipment on company property.

But compliance wasn't always as easy for smaller companies. For example, the government demanded that Lavabit—a secure email startup that allowed users, including Snowden, to encrypt messages—hand over the keys to Snowden's communications. Lavabit could not do so without exposing the information on all its customers and ultimately folded rather than comply.

There appear to be smaller ways to resist, though. "The government can request the information, but they can't compel how the information is given," says Twitter's general counsel, Vijaya Gadde. "You can make it easy or you can make it hard." Google also says it pushes back when a request is "overly broad." Pocketbook issues present a subtler means of resistance. FISA requires the government to reimburse companies for the cost of retrieving information. Google says that it doesn't bother to charge the government. But one company says that it uses that clause, hoping to limit the extent of the requests. "At first, we thought we shouldn't charge for it," says an executive of that company. "Then we realized, it's good—it forces them to stop and think."

Not just REVENUE was at stake. So were IDEALS that have sustained the TECH WORLD since the INTERNET exploded from a DEFENSE DEPARTMENT PROJECT.

In the end, though, there is a greater financial motive to cooperate. "Large companies do a lot of business with the government," one top technology executive points out. "It's hard to look at the government officers and say, 'We're fighting you on this—oh, and can I have that $400 million contract?'"

Tech companies also grew more vocal in their requests to publicize the number of FISA requests they received. They were only allowed to release reports that tally all government requests, including those from civil court and law enforcement. (The raw numbers, often in the low thousands, don't seem scary, but they lack context.) Google, Yahoo, Facebook, and Microsoft petitioned the FISA court to loosen the gags, and a long list of technology firms, including Apple and LinkedIn, submitted amicus briefs in support. But the government filed passionately opposing briefs and prevailed.

The clash illustrates a seemingly irresolvable conflict. While Silicon Valley must be transparent in many regards, spy agencies operate under a cloak of obfuscation. There is certainly a reason for the secrecy; evildoers who use an Internet service presumably might be less likely to keep using it if they were aware that the company was sharing communications with the NSA. But one of the disturbing consequences of secret programs is the destructive shroud of doubt they cast over everything they touch. Months after Snowden's leak, basic facts about Prism remain elusive. How much information is actually collected by the program? Exactly what kind of cooperation did the companies offer after those dates specified on that NSA PowerPoint slide? The companies contend that in addition to what they can't say, there's plenty they don't know.

"We're still guessing," says Richard Salgado, Google's director of information security and law enforcement. "We're not the author of those slides. We have no idea where they got some of that information."

"The question goes to issues of a highly classified nature," says Tekedra Mawakana, Yahoo's head of global public policy.

ALL SUMMER, the tech companies tried to deal with the fallout from Prism, while the NSA tried to figure out how to respond to the Snowden leaks. And then things got uglier for both sides.

In October, a Snowden leak exposed a program in which the NSA, without the knowledge or cooperation of the companies involved, managed to collect the address-book data of millions of people. *The Washington Post* reported that over the course of a single day, the NSA had collected "444,743 email address books from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail, and 22,881 from unspecified other providers." The practice was categorized internally at the NSA as an upstream method to collect data as it flows through the Internet, as opposed to downstream methods, like Prism, in which information was provided directly from the source. (In an earlier story about Prism, the *Post* printed a slide detailing the two approaches, which instructed analysts: "You should use both.")

Then Gellman and his *Post* team revealed documents detailing how the NSA, working with its British counterpart, GCHQ, had hacked into the traffic that moved exclusively on the private fiber connections linking the respective data centers of Google and Yahoo. The codename for this upstream program was Muscular.

In one sense, the news cleared up a mystery that had been baffling the companies. "It provided us a key to finally understanding what was going on," says Microsoft's general counsel, Brad Smith. "We had been reading about the NSA reportedly having a massive amount of data. We felt that we and the others in the industry had been providing a small amount of data. It was hard to reconcile, and this was a very logical explanation."

Still, news of the government raid on data-center traffic hit the industry with the visceral shock of having one's home robbed. The betrayal was most strikingly illustrated in a PowerPoint slide that showed how the NSA had bypassed Google's encryption, inserting a probe as data moved from its servers across the open Internet. Between two big clouds—one representing the public Internet, the other labeled "Google Cloud"—there was a little hand-drawn smiley face, a blithe emoji gotcha never meant to be seen by its victim. Google's Drummond wrote an indignant statement to the *Post*, describing the company as "outraged." Yahoo's director of security, Ramses Martinez, endorses the sentiment. "It was news to us," he says of Muscular. "We put a lot of work into securing our data."

It's one thing to object to a legal process that one believes is unconstitutional. It's quite another to be working for an American company, charged with protecting the privacy of customers, and find that the eyes staring across from you on the virtual Maginot Line of cyberdefense are those of the United States of America.

"At first we were in an arms race with sophisticated criminals," says Eric Grosse, Google's head of security. "Then we found ourselves in an arms race with certain nation-state actors [with a reputation for cyberattacks]. And now we're in an arms race with the best nation-state actors." Primarily, the US government.

But perhaps the most authentic expression of betrayal came from a relatively unknown Google security engineer named Brandon Downey in a post on his personal Google+ account. He prefaced his message by stating that he was speaking only for himself—but he might as well have been channeling his colleagues across the industry:

> *Fuck these guys.* ¶ *I've spent the last ten years of my life trying to keep Google's users safe and secure from the many diverse threats Google faces.* ¶ *I've seen armies of machines DOSing Google. I've seen worms DOS'ing Google to find vulnerabilities in other people's software. I've seen criminal gangs figure out malware. I've seen spyware masquerading as toolbars so thick it breaks computers because it interferes with the other spyware.* ¶ *I've even seen oppressive governments use state-sponsored hacking to target dissidents.* ¶ *... But after spending all that time helping in my tiny way to protect Google—one of the greatest things to arise from the internet—seeing this, well, it's just a little like coming home from War with Sauron, destroying the One Ring, only to discover the NSA is on the front porch of the Shire chopping down the Party Tree and outsourcing all the hobbit farmers with half-orcs and whips.*

Since the revelations, many companies have been beefing up their security. Google's Grosse had long pushed to implement encryption on data both as it moved across public networks and within the company's data centers—a tactic the company had begun to pursue. "We were partway through deploying when we learned how far the NSA had gotten," Grosse says. "The hypothetical thing we were worried about was finally happening."

Yahoo, which has lagged in adopting additional encryption, vows to strengthen it, including on traffic between its data centers, by the end of March. "There is nothing more important to us than protecting our users' privacy," CEO Marissa Mayer said in a statement. Facebook and Microsoft plan to phase in a technique called Perfect Forward Secrecy, which drastically limits the information an intelligence agency might be able to access by using many more secret keys to encode data. (Google and Twitter already use it.) Previously, cracking a single cryptographic key would open a treasure trove of information, but with forward secrecy, even sophisticated cryptoanalysis gets you only a small portion of the loot. The point of such measures, wrote Microsoft's Smith in a blog post, was to ensure that government access to data is "decided by courts rather than dictated by technological might."

But even strong encryption won't necessarily keep out the NSA. Another Snowden-generated scoop, this one a collaboration between ProPublica and *The New York Times*, detailed the agency's spectacular recent success in cracking popular forms of cryptography. The tactics include using purloined or company-supplied keys to decode all the messages of a major Internet service and exploiting unreported vulnerabilities in software systems. Some documents raised the possibility—already suspected by some in the crypto community—that the NSA helped promote weak encryption standards that it knows how to crack. It is a well-known principle of cybersecurity that any flaw will eventually be discovered and exploited. If in fact the NSA was not reporting known security holes, then it risked exposing domestic information and secrets to evildoers. It may even have allowed foreign governments to snatch high-value corporate secrets.

"The NSA is willing to compromise the security of *everything* to get what they want," security expert Bruce Schneier says.

"Think about the damage this does to America," says US Representative Rush Holt (D-New Jersey) who is the rare member of Congress with a PhD in physics—and one of a number of legislators pursuing measures that would curtail the NSA's activities. "The NSA is saying, 'We've got to make sure the encryption has flaws so we can decrypt.' Isn't that the pinnacle of arrogance? *No one else knows how to do it or is as smart as we are. They won't realize we've degraded our product.* But the truth always comes out. And America is worse off because of it."

Certainly the tech companies felt worse off. In November, the German newsweekly *Der Spiegel*—another recipient of Snowden leaks—described an NSA/GCHQ exploit that seemed tailor-made to erode trust. In an attempt to gain access to the Brussels-based telecommunications firm Belgacom, the agencies set up bogus versions of sites like Slashdot and LinkedIn. When employees tried to access the sites from corporate computers, their requests were diverted to the phony replicas, which the spies used to inject malware into their machines.

Using considerable understatement, LinkedIn's general counsel, Erika Rottenberg, says, "We are not happy that our intellectual property is being used in that way." It is not hard to see why. If foreign customers can't know whether they are using a legitimate social network or a spy-created fake, they are liable to log off altogether.

For years, companies from espionage-happy countries like China have been spurned by overseas buyers who didn't trust their products. Now it's America's turn. And that is already having an impact on young companies looking to grow internationally. "Right now, our ad business is 95 percent US-based," says David Karp, founder of Tumblr. "As we start to take this business overseas, we're running up against stricter EU laws, particularly on privacy, as part of their reaction to US practices on the Internet."

"The other day I saw my first pitch that exploited the situation," says Brad Burnham, a managing partner at Union Square Ventures. "It was a Dropbox clone that told us, 'We're in Europe and we have a government that doesn't snoop!'" Though the major companies have not yet reported losing large amounts of business, they do acknowledge that their overseas customers are worried. Forrester Research estimates that as much as $180 billion could be lost due in large part to overseas companies choosing not to patronize the American-based cloud. "American companies are feeling shellacked by overeager surveillance," says US senator Wyden. "It reduces our competitiveness in a tough global economy."

Even so, a decline in trust, or even business, is not the tech companies' biggest worry in the post-Snowden era. Facebook CEO Mark Zuckerberg believes that the inherent value of the Internet will keep his users coming to the big online services. But he is among those who fear that the NSA revelations have unleashed a potential backlash from other nations that could hurt not only those companies but the net itself. "Part of the reason the US blew it is that governments around the world are now threatening the security of the Internet by passing their own laws that permit intrusions on Internet users," he says.

Zuckerberg is referring to a movement to balkanize the Internet—a long-standing effort that would potentially destroy the web itself. The basic notion is that the personal data of a nation's citizens should be stored on servers within its borders. For some proponents of the idea it's a form of protectionism, a prod for nationals to use local IT services. For others it's a way to make it easier for a country to snoop on its own citizens. The idea never posed much of a threat, until the NSA leaks—and the fears of foreign surveillance they sparked—caused some countries to seriously pursue it. After learning that the NSA had bugged her, Brazilian president Dilma Rousseff began pushing a law requiring that the personal data of Brazilians be stored inside the country. Malaysia recently enacted a similar law, and India is also pursuing data protectionism.

> "The US needs to help FIX THIS PROBLEM," Facebook CEO Mark Zuckerberg says, worried about the advent of multiple "SPLINTERNETS."

To most people familiar with Internet protocols, this sounds crazy. Google's Drummond refers to the result—dozens of independent Internets that don't communicate with one another—as "splinternets." "It's not realistic and very shortsighted," LinkedIn's Rottenberg says. "How is that even implemented? If I'm a Brazilian resident and I'm traveling, I can't get my data?"

It's not just developing economies that are considering this route. In Germany, where the NSA bugged the phone of chancellor Angela Merkel, there is talk of a similar scheme, called Schengen routing. René Obermann, chief executive of Teutonic giant Deutsche Telecom, seemed to endorse the principle at a European cybersecurity conference. In the pre-Snowden world, such a proposal would have been hooted down. But now Obermann was speaking to an audience that was all but armed with pitchforks, ready to storm the listening posts of American spooks.

"The Internet was built without reference to international borders, and that has allowed for huge innovation," Yahoo's Mawakana says. "But how does it function when countries try to pin the cloud to the ground? What if Indonesia pins, Brussels pins, and Brazil pins? Will companies invest equally across the world?"

One of the worst effects could be to dampen the prospects of startup companies. Would Facebook or YouTube ever have gotten off the ground if they had to figure out how to store their data in dozens of different countries? "More and more markets, like Brazil, are working on passing laws that would basically say, 'You can't do business here unless you physically house user data in our country,'" Karp says. "That's an incredibly expensive proposition for Tumblr, but it's *impossible* for the aspiring young company that wants to build something for everyone to use over the entire world."

"The US needs to help fix this problem," Zuckerberg says. But the Obama administration worries that any US government attempts to do so will only fortify the resolve of other nations to balkanize—to prove that they will not be bullied. So it's up to the industry to make the case.

Previously, companies could argue that balkanization would

give the citizens of those artificially isolated countries less choice and more censorship and snooping. But that's a hard sell now that Snowden has revealed that the US—through its tech companies—is the one snooping on the rest of the world.

"THIS ISN'T THE COMPANIES' fault. They were compelled to do it. As a nation, we have a responsibility to stand up for the companies, both domestically and internationally. That is our nation's best interest. We don't want our companies to lose their economic capability and advantage. It's for the future of our country."

Those words could have come from a policy spokesperson for Google, Facebook, Microsoft, or Yahoo. Or one of the legislators criticizing the NSA's tactics. Or even a civil liberties group opposing the NSA. But the source is US Army general Keith Alexander, director of the NSA. Still, even as he acknowledges that tech companies have been forced into a tough position, he insists that his programs are legal, necessary, and respectful of privacy.

The NSA is legendarily tight-lipped, so much so that for decades it refused to publicly acknowledge its own existence. But, in one of the less heralded consequences of the Snowden revelations, it has apparently realized that it must defend itself to the press. And so, on a crisp day in early November, I am invited to visit its imposing glass-walled headquarters in Fort Meade, Maryland. After submitting my personal data—including the serial number of my tape recorder—I pass through three security checkpoints and park my car in a specified space. Eventually I take a seat in a conference room bedecked with patriotic posters that trumpet national security and privacy. I am introduced to general counsel Rajesh De; Anne Neuberger, the NSA's point person for partnerships with the private sector; and Rick Ledgett, a deputy director who heads the agency's Media Leaks Task Force, a position created last summer for Snowden damage control.

And then the top man enters, a surprise participant who wants to set the tone for the interview, staying for the first 20 minutes of a session that will last more than two hours. Trim in physique and efficient in expression, Alexander has a charismatic confidence that clearly has aided him in ascending to a key role in national security.

"That program, by itself, is the hornet's nest," Alexander says in reference to Prism. "It is the hornet's nest that [enables] the NSA to see threats from Pakistan and Afghanistan and around the world, share those insights with the FBI—who can look inside the United States, based on their authorities—and find out, is there something bad going to happen here?" Alexander cites the case of Najibullah Zazi, the radical Islamist who planned to bomb the New York City subways in 2009, implying that information collected under the Prism program led to his capture.

"My concern is that, without knowing the facts, people will say, 'Let's put that hornet's nest away.' *We* sure would like to get rid of that hornet's nest. We would like to give it to somebody else, anybody else. But we recognize that if we do that, our nation now is at greater risk for a terrorist attack. So we're going to do the right thing; we're going to hold on to it, let people look at the options. If there is a better option, put it on the table."

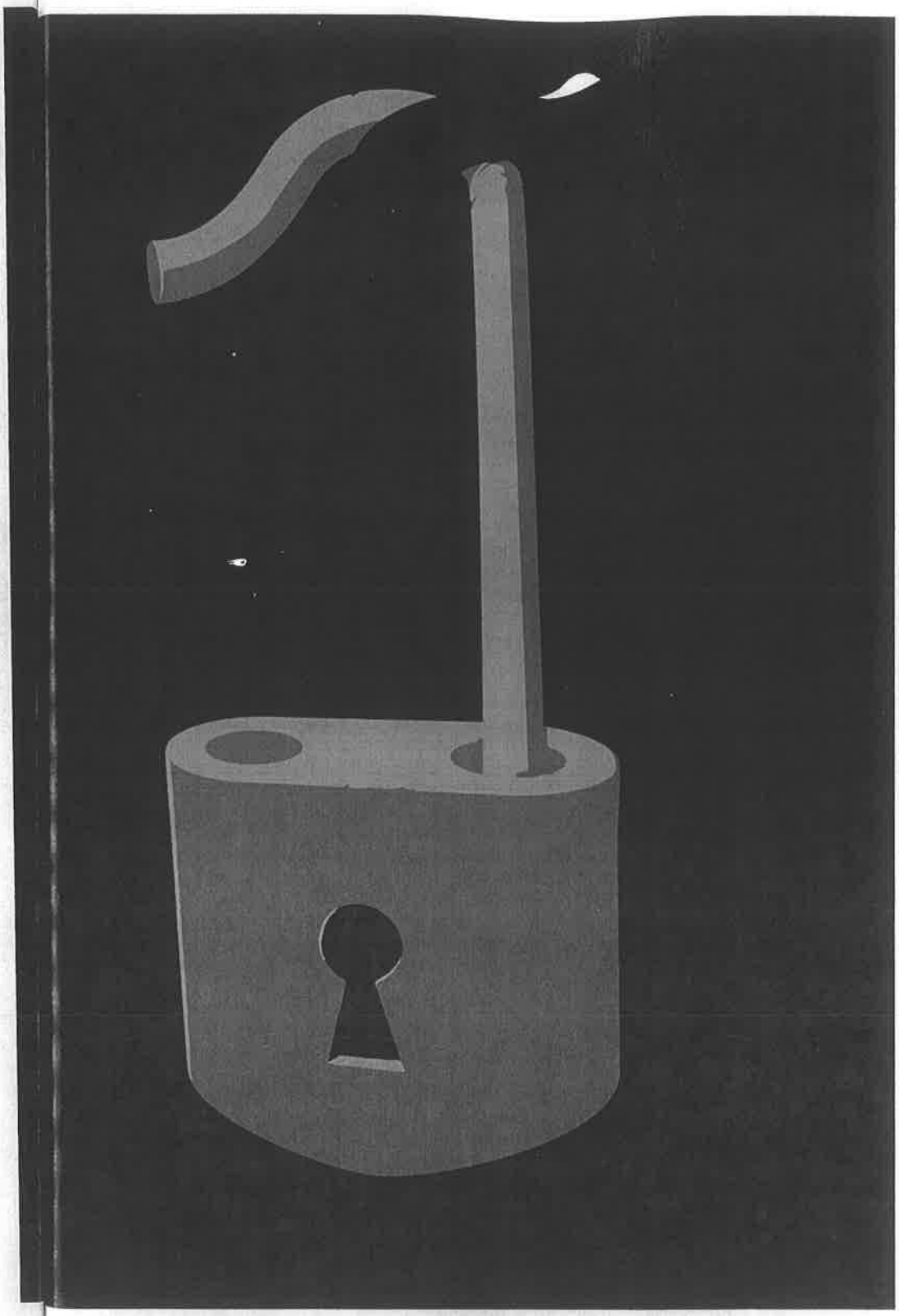
Oddly, at heart, the NSA's complaints sound remarkably similar to those of the tech companies: *People don't understand us.* "No one knows how the NSA works," Ledgett says. "It's always been a black box, *Enemy of the State* movies, stuff like that. People don't understand the NSA's checks and balances."

That's one of the key points these officials want to make: While the NSA might collect a lot of data, rules and oversight limit the extent to which privacy is compromised. In an earlier speech, Alexander said, "You need the haystack to find the needle." Simply gathering the haystack is benign, the officials claim, because ample protections exist to constrain any searches of that information. De refers to the comprehensive collection of voice call metadata as "one of the most highly regulated programs in the entire federal government." He describes in detail the multiple times it has been reauthorized in Congress and the courts, the limited number of people who have access to it, and the oversight employed to make sure that they use it as directed. (In December a federal judge ruled that the collection of phone metadata is likely unconstitutional, but stayed his order pending appeal.)

Similar controls exist for Prism, which the NSA views as its most important tool. "Gmail is the most popular terrorist mail service in the world," one official says. "Second place is Yahoo. It's not because Google and Yahoo are evil, it's because they offer a great service."

Exactly how much information the NSA ultimately collects with Prism it won't say. According to the Snowden leaks, on April 5, 2013, there were 117,675 "records" in the Prism database. If these targets have contact with people inside or associated with the United States, Prism can wind up collecting tons of information about Americans. Between Prism and upstream collection procedures like Muscular, the NSA winds up with plenty.

For years, companies from ESPIONAGE-HAPPY COUNTRIES like CHINA have been spurned by OVERSEAS BUYERS who didn't trust their products. NOW IT'S AMERICA'S TURN.



"The NSA is **willing to compromise the security of everything** to get what they want," one cryptographer says.

CHRISTOPH NIEMANN

Ledgett identifies several steps by which the NSA winnows data to exclude Americans' email, search queries, and selfies. "We are responsible for minimizing the collection of US personal information," he says. However, this process so far has been largely self-regulated, and recent declassified FISA court documents indicate that the NSA has fallen short on multiple occasions; the court has criticized the NSA for overcollecting or failing to properly filter its content.

The officials paint a picture, though, of a system that fundamentally works. They describe a rigorous training process. They tell me that respect for boundaries is drilled into the psyche of NSA employees from the day they are hired. (As for one embarrassing incident, in which employees tracked their romantic partners, the officials emphasize its rarity—and point out that the abuses were caught by the NSA's own system of frequent polygraph tests.) Ledgett provides an example of what happens when someone's information is mistakenly analyzed. The agency, he says, had tracked a high-value target in South Asia for over a decade before learning that he had once applied for a green card—making him, under NSA rules, a "US person." "As soon we discovered that," Ledgett says, "we dropped collection on him under our Executive Order 12333 authority and canceled 14 years of reports."

Critics charge that while there is not yet any evidence of massive abuse of the NSA's collected data, there is also no guarantee that a future regime won't ignore these touted protections. These officials discounted that possibility, saying that the majority of NSA employees wouldn't stand for such a policy. "If that happened, there would be lines at the Inspector General's office here, and at Congress as well—longer than a Disneyland line," Ledgett says. (The fates of several NSA employees-turned-whistleblowers indicate that anyone in that hypothetical queue would be in for a ride far wilder than anything in Anaheim.)

The NSA acknowledges that news of its activities has put US technology companies in a bind. But the solutions are elusive, even for a seemingly easy problem like letting companies share more detail about the national security requests they receive. "We have a shared interest in trans-

parency," says general counsel De, who adds that the NSA is preparing its own report to disclose the total number of requests and user accounts from all companies combined. Yet the NSA continues to oppose efforts to break down the numbers: It might provide a road map for enemies to use the least scrutinized services.

The officials profess not to worry about companies using stronger cryptography to protect users from intruders—including those in Fort Meade. "We applaud the use of encryption," Neuberger says. "We support better security." But they imply that if the techniques make the NSA's job more difficult, the agency might miss vital clues.

And the NSA insists that, despite the implications of those Snowden-leaked documents, it does not engage in weakening encryption standards. "The same standards we recommend are the standards we use," Ledgett says. "We would not use standards we thought were vulnerable. That would be insane." The officials won't deny the NSA's use of software vulnerabilities but portray their general behavior as protective.

"We are heavily biased toward defense," Ledgett adds, citing one case in which the NSA discovered a serious vulnerability in one company's software that could have impacted users all over the world. "We talked about it for a few days internally and decided it was so critical to the entirety of the US government and most of America that we disclosed [the vulnerability to that company]. We could have made hay on that forever on a huge range of targets."

During the conversation, the officials could barely contain the frustration they feel about how the world—and their fellow Americans—views them post-Snowden. They have read Brandon Downey's heartbroken lament about his own government breaking into his beloved data center. They understand that journalism conferences routinely host sessions on protecting information from government snoops, as if we were living in some Soviet society. And they are aware that multiple security specialists in the nation's top tech corporations now consider the US government their prime adversary.

But they do not see any of those points as a reason to stop gathering data. They chalk all of that negativity up to monumental misunderstandings triggered by a lone leaker and a hostile press. NSA employees see themselves as dealing with genuine deadly threats to the nation, and it makes them crazy when people assume that spooks at Fort Meade are intent on stealing their privacy.

"It's almost delusional," Ledgett says. "I wish I could get to the high mountaintop to scream, *'You're not a target!'*"

THE PROBLEM, of course, is not merely one of misunderstanding. It is largely a consequence of the inexorable rise of digital technology. In a sense, the tech companies are more like the NSA than they would like to think. Both have seized on the progress in computing, communications, and storage to advance their respective missions. (When you think of it, Google's original mission statement—"to collect and organize the world's information"—might also apply to the activity at Fort Meade.) Both have sought to fulfill those missions by amassing huge troves of personal information—and both offer trade-offs that seemingly justify the practice. Google, Facebook, and others argue that they can use that information to improve the lives of their customers far in excess of any discomfort that may come from sharing that data. The NSA believes that it's necessary to draw on that information to prevent a replay of 9/11 or worse. Both have established elaborate self-policing procedures to minimize abuse and claim to strictly follow the external constraints that limit their activities. When either makes a mistake, it invariably vows to do better—at least when its overreaches become public. Of course, the comparison goes only so far. If the NSA doesn't connect the dots, the door is open to catastrophe.

Throughout the fall, legislators introduced a number of bills that would demand more transparency and oversight, or even outlaw the collection of bulk information altogether. The tech companies have been lobbying Congress to get at least some of those provisions into law. In December they specified their preferences—including no bulk data collection of Internet communications—in an open letter, then forcefully stated their case in a meeting with President Obama. The next day, the White House released a 300-page report from the advisory panel he had appointed to review NSA practices. "Free nations must protect themselves," the report stated, "and nations that protect themselves must remain free." Its 46 recommendations call for tempering the breadth of NSA activities to accommodate privacy concerns, revealing more NSA operations to outside scrutiny, engaging in bulk data collection only when justified by concrete national security concerns, and refraining from some of the dark-side hacker practices that erode confidence in private tech.

But civil liberties groups were disappointed that the panel did not make a stand against bulk data collection. At least one suggestion—that bulk personal data be retained by companies instead of the government—might present a headache for the tech industry. Would Google, Facebook, and similar firms be seen as archivists for spies?

The president has indicated that early this year he would identify which recommendations he would endorse. (Some would require legislation.) While the programs in question may have begun under the previous administration, Obama has made it clear that he is not giving up his 702s. "As the president has said, FISA is an important tool in our effort to disrupt terrorist plots," Caitlin Hayden, a National Security Council spokesperson, wrote in a statement to WIRED. "He believes that there are steps we can take to give the American people additional confidence that there are added safeguards against abuse, including putting in place greater oversight, greater transparency, and further constraints on the use of this authority."

Nicole Wong, the nation's deputy chief technology officer (and former chief privacy lawyer for Google), emphasizes the government's good intention: "We're trying to prevent another Boston bombing," she says. "In a world where we have those threats, what can we live with? Is it more transparency, is it less collection?"

There are others who argue that we may regret even modest constraints on the NSA. Former Microsoft research head Nathan Myhrvold recently wrote a hair-raising treatise arguing that, considering the threat of terrorists with biology degrees who could wipe out a good portion of humanity, tough surveillance measures might not be so bad. Myhrvold calls out the tech companies for hypocrisy. They argue that the NSA should stop exploiting information in the name of national security, he says, but they are more than happy to do the same thing in pursuit of their bottom lines. "The cost is going to be lower efficiency in finding terrorist plots—and that cost means blood," he says.

That's the way the government sees it too. In a white paper last summer, the Obama administration argued that collecting the details of everyone's phone behavior is justified, because the program is about "forward-looking prevention of the loss of life, including potentially on a catastrophic scale."

But even if the spy programs are viewed as justified, and whether they are tempered or not, we're still left with the most sickening aspect of the Snowden revelations: The vast troves of information gathered from our digital activities will forever be seen as potential fodder for government intelligence agencies. A lot of people became inured to worries about Little Brother—private companies—knowing what we bought, where we were, what we were saying, and what we were searching for. Now it turns out that Big Brother can access that data too. It could not have been otherwise. The wealth of data we share on our computers, phones, and tablets is irresistible to a government determined to prevent the next disaster, even if the effort stretches laws beyond the comprehension of those who voted for them. And even if it turns the US into the number one adversary of American tech companies and their privacy-seeking customers.

"I was naive," says Ray Ozzie, who as the inventor of Lotus Notes was an early industry advocate of strong encryption. "I always felt that the US was a little more pure. Our processes of getting information were upfront. There were requests, and they were narrow. But then came the awakening," he says. "We're just like everybody else."

For the latest NSA news and analysis, go to WIRED.com/nsa.