BUSINESS REPORT

Spies, Technology, and Business

How the NSA eavesdropping scandal could balkanize the Internet or make it safer.

CONTENTS

Read the report online at technologyreview.com/business

DANIEL ZENDER

The Big Question

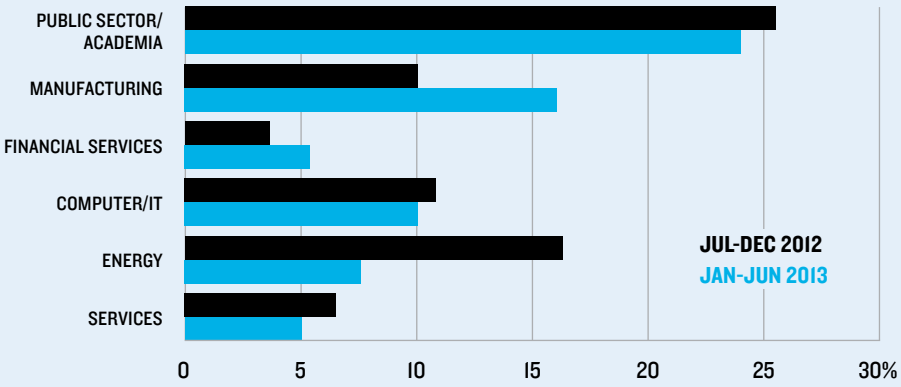
Spying Is Bad for Business

Can we trust an Internet that's become a weapon of governments?

● Following a one-day summit in Brasilia this February, negotiators from Brazil and Europe reached a deal to lay a $185 million fiber-optic cable spanning the 3,476 miles between Fortaleza and Lisbon. The cable will be built by a consortium of Spanish and Brazilian companies. According to Brazil's president, Dilma Rousseff, it will "protect freedom." No longer will South America's Internet traffic get routed through Miami, where American spies might see it.

She's not being paranoid. Documents leaked last June by former U.S. intelligence contractor Edward Snowden revealed a global surveillance operation coördinated by the U.S. National Security Agency and its counterpart in Britain, the GCHQ. Among the hundreds of millions of alleged targets of the dragnet: Brazil's state oil company, Petrobras, as well as Rousseff's own cell phone. →

Top Targets of Cyberattacks



The big question in this *MIT Technology Review* business report is how the Snowden revelations are affecting the technology business. Some of the consequences are already visible. Consumers are favoring anonymous apps. Large Internet companies, like Google, have raced to encrypt all their communications. In Germany, legislators are discussing an all-European communications grid.

Eugene Kaspersky, founder of the Moscow-based antivirus company that bears his name, warns that the Internet is fracturing. His view is that Brazil's new cable is akin to China's Great Firewall (that country's system for censoring Web results), or calls by nationalists in Russia to block Skype, or an unfolding German plan to keep e-mail traffic within its borders. Nations are limiting access to their networks. Kaspersky's company predicts that this could lead to "the collapse of the current Internet, which will break into dozens of national networks."

Analysts including Forrester Research predict billions in losses for U.S. Internet services such as Dropbox and Amazon because of suspicion from technology consumers, particularly in Europe, in the wake of Snowden's revelations. "The Snowden leaks have painted a U.S.-centric Internet infrastructure, and now people are looking for alternatives," says James Lewis, director of the strategic technologies program at the Center for Strategic and International Studies in Washington, D.C.

Many nations eavesdrop, each for their own reasons. Some target dissidents with malware to watch their keystrokes. Others, like China, also bleed companies of intellectual secrets about jet fighters and wind turbines. So pervasive and successful has digital espionage become that in 2012, Keith Alexander, the Army general in charge of the NSA, described it as "the greatest transfer of wealth in history." He estimated that U.S. companies lose $250 billion a year to intellectual-property theft.

The Snowden leaks painted a picture of a U.S.-centric Internet. Now people are looking for alternatives.

This is hastening the trend to secure networks, to isolate them, or even to disconnect. In this report, we visit a small energy company for which a network cable might as well be Medusa's hair. The company is so frightened that it keeps its best ideas on computers quarantined from the Internet. Retrograde technology is winning money and resources. Following the Snowden revelations, Russia's secret service placed an order for $15,000 worth of typewriters and ribbons. They said paper was safest for some presidential documents.

Security experts have been warning for some time that computer networks are not secure from intruders. But in 2013, we learned that the mayhem has become strategic. Governments now write computer viruses. And if they can't, they can purchase them. A half-dozen boutique R&D houses, like Italy's Hacking Team, develop computer vulnerabilities and openly market them to government attackers.

Criminals use common computer weaknesses to infect as many machines as possible. But governments assemble large research teams and spend millions patiently pursuing narrow objectives. Costin Raiu, a Kaspersky researcher who investigates such "advanced persistent threats," says he logs on to his computer assuming he is not alone. "I operate under the principle that my computer is owned by at least three governments," he says.

That is a threat mainstream technology companies are grappling with. The U.S. government circumvented Google's security measures and secretly collected customer data. British spies scooped up millions of webcam images from Yahoo. In December, on Microsoft's official blog, the company's top lawyer, Brad Smith, said he had reason to view surreptitious "government snooping" as no different from criminal malware. Microsoft, along with Google and Yahoo, has responded by greatly widening its use of encryption.

"We're living in a very interesting time, where companies are becoming unwilling pawns in cyberwarfare," says Menny Barzilay, a former Israeli intelligence officer now working in IT security for the Bank Hapoalim Group, in Tel Aviv. In this new context, nobody can say where the responsibilities of a company may end and those of a nation might begin. Should a commercial bank be expected to expend resources to defend itself when its attacker is a country? "This is not a 'maybe' situation. This is happening right now," says Barzilay. "And this is just the beginning."

If the Internet and its components cannot be trusted, how will that affect business? Consider the case of Huawei, the Chinese company that last year became the world's largest seller of telecom equipment. Its U.S. market share is paltry, because the

SOURCE: SYMANTEC

government has long claimed that Huawei's gear is a Trojan horse for China's intelligence services. Now American firms like Cisco Systems say their Chinese customers are turning away for similar reasons. After all, the Snowden documents suggest how vigorously the NSA worked to insert back doors in gear, software, and undersea cables—in some cases via what the agency called "sensitive, cooperative relationships with specific industry partners" identified by code names.

Mistrust is also creating business opportunities. In this issue we travel to an old bunker in Switzerland that local entrepreneurs have turned into a server farm, hoping to do for data what the Swiss once did for Nazi gold and billionaires' bank accounts. Thanks to its privacy laws and discreet culture, the country is emerging as a hub for advanced security technology. In Lewis's view, these sorts of technological initiatives threaten the American lead in Internet services such as remote data storage. "It hasn't been long enough to know if the economic effects are trivial or serious, but the emergence of foreign competitors is a sign that it's serious," he says.

There's even a shift under way in consumer technology. Consumers have been rushing to download texting apps like Snapchat, where messages disappear. They are posting on anonymous message boards like Whispr and buying "cryptophones" that scramble their calls. Spy-shop stuff is going mainstream. Phil Zimmerman, a famous privacy advocate, helped create one of the cryptophones, the $629 Blackphone, launched in February at the big mobile communications conference in Barcelona, Spain.

That is how Edward Snowden is affecting business. People are asking questions about technology products, and technology companies, that they never asked before. Is it safe to connect? Are you Russian or American? "This is something that changed since last June, when the leaks started," says Mikko Hypponen, chief research officer of the Finnish security company F-Secure. "Before, the idea was that the Web had no borders, no countries. This was the naïve utopia. Now we have woken up." *—Antonio Regalado*

Emerged Technologies

Cyberspying Targets Energy Secrets

Intruders seek data on oil deposits, cutting-edge technology.

● Take a tour of 1366 Technologies, a startup near Boston that is developing a cheaper way to make solar cells, and you will see open spaces with low cubicles, engineers at their desks, a machine shop, and testing equipment running silicon wafers through their paces.

But the tour is a bluff: it's what you don't see that's really interesting. In another part of the building—one with no obvious way in—sit the engineers working on the core technology, machines that could cut the cost of silicon wafers for solar cells in half. Perhaps most important, computers used for the real work are entirely cut off from the Internet.

"We are paranoid," 1366 CEO Frank van Mierlo says. "We've taken our entire engineering server offline and air-gapped it, like the Department of Defense."

There has recently been much talk in Washington about the need to guard critical infrastructure, such as power plants, against possible enemy cyberattacks. But energy companies say that their key inventions and business data are already the target of increasingly sophisticated cyper-espionage.

"[It] quietly kept getting worse and worse," Dana Deasy, the former chief information officer of BP, said last November during a meeting of information technology executives in Barcelona, Spain. "You finally wake up one day and you're sitting in a world where this is a serious threat to the industry as a whole."

Attacks can go unnoticed for years, or are never reported. As a result, estimates of stolen intellectual property vary "so widely as to be meaningless," according to a 2011 report on foreign cyberspying by the U.S. Director of National Intelligence, which cited calculations of between $2 billion and $400 billion a year.

Companies say they worry most about state-sponsored attacks, which tend to be "incredibly well organized, incredibly sophisticated," according to BP's Deasy.

$800 million
Spying damage to one U.S. company

Some of the hackers are looking for proprietary data about oil fields, painstakingly gathered using costly seismic surveys, which underpins a business worth $3 trillion a year. Adam Segal, a fellow for China studies at the Council on Foreign Relations, says stolen survey data is believed to have influenced bidding on Iraqi oil fields.

Attackers leave clues but are rarely caught. In 2011, the security firm McAfee described "operation Night Dragon," a series of computer intrusions at oil and

Invisible Threat
Recent cyberattacks on energy companies have gone unsolved

	Discovered	Suspected Source	Target
Stuxnet	2010	U.S./Israel	Iran's nuclear facility
Night Dragon	2010	China	Oil exploration data
Energetic Bear	2012	Russian Federation	Energy companies in 10 countries
Shamoon	2012	hacktivists	Saudi Aramco computers

SOURCE: MCAFEE, CROWDSTRIKE; MIT TECHNOLOGY REVIEW

gas companies that they traced to China. Researchers at CrowdStrike have been tracking an "adversary group" they call Energetic Bear, based in the Russian Federation, which strikes western energy firms by installing malware that collects passwords. The United States allegedly spied on the Brazilian state oil giant Petrobras.

Few companies will admit they've been the victims of espionage. One that did is American Superconductor. In 2011, the Massachusetts company sued its largest customer, the Chinese wind-turbine maker Sinovel, saying it had stolen its key technology, a way of making it easier for wind turbines to integrate with the electricity grid.

In August, a federal grand jury indicted Sinovel, alleging that it had offered money and an apartment in Beijing to induce an American Semiconductor employee to e-mail the source code for the technology to China. American Superconductor says it lost $800 million in revenues and its stock cratered, falling more than 75 percent.

The case points to how intellectual-property theft often relies not only on sophisticated computer attacks but also on insiders. But it justifies the care that 1366 takes, says CEO Van Mierlo: "You only have to listen to the horrible stories of American Superconductor to know how damaging this stuff can be." —*Kevin Bullis*

Emerged Technologies

Before Snowden, There Was Huawei

The travails of a Chinese telecom company show how spying charges could hurt U.S. firms.

● How's this for a tough sales job? The American sales reps of Huawei offer top-notch telecom gear at a 35 percent discount. But anytime they get near to closing a sale, their customers get a visit from the FBI or the U.S. Department of Commerce.

The message from the feds isn't subtle: buy something else.

Huawei, based in Shenzhen, China, is the world's largest seller of telecom equipment, commanding 20 percent of the market. Yet it is barely a factor in North America. Here its market share in optical equipment is just 1.4 percent, and in switches and routers it's just 0.1 percent.

Just as Huawei has been shut out of the American market, leaks about the pervasiveness of spying by the NSA and other U.S. intelligence agencies might now hurt American companies abroad. Businesses are starting to talk of a "Snowden effect" of lost sales, dimmed prospects, and growing uncertainty, as they too come under a cloud of mistrust.

The U.S. worried that the Chinese government could be using commercial telecom gear to eavesdrop. No wonder. It appears American spies were doing the same.

Huawei (pronounced *wah-way*) was founded in 1987 by Ren Zhengfei, a former military officer who splits the CEO job with executives who rotate every six months. As Huawei expanded overseas, suspicions began to swirl around the company, particularly in the United States. Its effort to buy 3Com, a networking company, was blocked by a trade panel that assesses national security risks. In 2011, Cisco Systems, a competitor, developed talking-point slides that laid out reasons for "Fear of Huawei."

In 2012, partly at the Chinese company's request, the U.S. House Intelligence Committee investigated and released a report. It offered no real proof of spying, yet it still concluded that the United States must "view with suspicion" progress by Chinese companies in the North America telecommunications market.

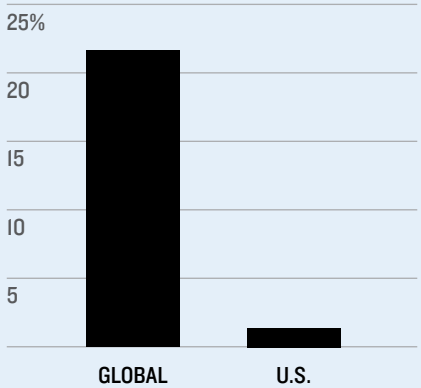
The concern was that somehow, with Huawei's knowledge or without it, the Chinese government could use equipment sold by the company to eavesdrop or even to gain an advantage in a cyberwar. Huawei loudly denied the charges; it cried "discrimination."

The irony now is that leaked National Security Agency documents suggest the U.S. was doing everything it suspected China of. The documents indicate that the U.S. may have compromised routers from Cisco, Juniper, and Huawei. It's also believed to have weakened encryption products so the ciphers used by commercial software could be broken.

The companies named in those leaks all deny knowing of the backdoors. All say they are investigating. But the loss of trust is hurting U.S. companies. In December, Cisco said the allegations caused a significant drop in sales in China. "It's causing people to stop and then rethink decisions," Robert Lloyd, Cisco's president of development and sales, told investors. IBM's hardware sales in China plunged 40 percent in the financial quarter following the leaks.

Huawei can feel vindicated, but only to a degree. Its sales haven't picked up in the U.S., and now some alarmed European countries may also be reconsidering Chinese gear. "There's a universal lack of trust,

Closed Out
How mistrust of China shapes Huawei's market share



SOURCE: OVUM; REFERS TO OPTICAL TELECOMMUNICATIONS EQUIPMENT

and now we have a pretty obvious proof point of that," says William Plummer, Huawei's spokesman in Washington, D.C. As it turns out, everyone's gear is vulnerable. "We've been saying that for years," says Plummer.

In several white papers, Huawei has outlined what it thinks are ways to improve security by adopting common standards and, perhaps, checks by third parties. James Lewis, an analyst at the Center for Strategic and International Studies, describes the challenge ahead as "how to build trusted networks from untrustworthy components."

But the bigger fallout may be a rise in protectionism. "It's been mostly open competition since the beginning of the Internet, and the companies that did well are the ones that won the competitions," says Lewis. Now, with escalating security worries, countries may take the chance to stack the deck against foreign competitors or build up their own industries.

"The overall effect will be bad for the whole global economy," says Lewis.

—Antonio Regalado

Emerged Technologies

Spinoffs from Spyland

How America's eavesdropping agency commercializes technology.

● It takes more than a little tradecraft to spin off a startup from the National Security Agency.

Chris Lynch, an investor with Atlas Venture, knows this firsthand. Two years ago, he spent weeks trying to sign a deal with nervous NSA programmers who not only were sworn to secrecy but were barred from carrying cell phones at work. There were furtive Skype conversations and parking-lot phone calls that would end after strange clicks.

Eventually, $2 million in seed money was enough to lure five programmers from the NSA. These days they're working at Sqrrl, a company in Cambridge, Massachusetts, that's selling a commercial version of the database behind some of the spy agency's most controversial eavesdropping programs.

"These guys were government hacks working in a cave, and in a highly structured environment," says Lynch. "Kind of the opposite of an entrepreneur."

A blistering public debate surrounds the NSA's secret eavesdropping programs. But what's less well known is that the agency actively patents inventions and contributes to open-source projects, and that its employees occasionally—so far, very occasionally—emerge from secrecy to create spinoff companies.

Like other federal agencies, the NSA is compelled by law to try to commercialize its R&D. It employs patent attorneys and has a marketing department that is now trying to license inventions like tamper-proof bags, secure manhole covers, and a "dispersion system" to make sure shredded documents can't be pieced back together. One startup, Integrata, based in Maryland, exclusively licensed a patent on how to detect intruders on wireless networks.

Revelations about the extent of NSA spying have only increased demand for just the sorts of technology the agency excels at. And at least one NSA offshoot is developing products expressly to defeat the agency's snooping.

"We believe government surveillance has gone too far and individuals have lost their right to privacy," says Will Ackerly, who spent eight years building software for the NSA before founding Virtru, a Washington, D.C., company selling a secure file-sharing system that he says could defeat mass surveillance. Ackerly says he took another seven NSA engineers and contractors with him—about half the staff at his startup.

The NSA is one of 16 U.S. government organizations devoted to intelligence gathering (among them, only the CIA is larger). It has a budget of $10.5 billion a year, of which about $500 million is spent on more basic R&D in programming, optics, microelectronics, and quantum computing. The agency claims more than 170 patents, and it is even said to have invented the audiocassette.

16
Number of U.S. intelligence agencies

But the NSA has faced severe challenges trying to keep up with rapidly changing technology. Back in 1999, a new director, Michael Hayden, began efforts to shed aging spies after scathing reports that the agency was stuck in the "Telex age." It had failed to predict an Indian nuclear test and couldn't intercept North Korean signals because they were sent along fiber-optic cables, not over the air.

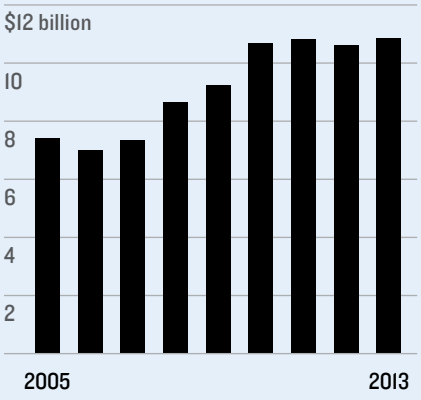
Most recently, the NSA's revamp included a sweeping effort to dismantle hundreds of single-purpose databases, or "stovepipes," and switch to flexible cloud computing, where data is spread across thousands of servers. In fact, in 2008, NSA brass ordered the agency's computer

Meet the NSA Spinouts
Startup companies based on technology from the National Security Agency

Integrata Security	Baltimore	$540,000 raised	Wireless monitoring systems
KeyW	Hanover, MD	Publicly traded	Geospatial intelligence
Six3 Systems	McLean, VA	Acquired	Surveillance solutions
Sqrrl	Cambridge, MA	$7.2 million raised	Enterprise databases
Fixmo	Toronto	$4I million raised	Mobile security

SOURCE: MIT TECHNOLOGY REVIEW

The NSA's Budget



and information sciences research organization to create a version of the system Google uses to store its index of the Web and the raw images of Google Earth.

That team was led by Adam Fuchs, now Sqrrl's chief technology officer. Its twist on big data was to add "cell-level security," a way of requiring a passcode for each data point in a spreadsheet. At the NSA, that's how software (like the infamous PRISM application) knows what can be shown only to people with top-secret clearance. Similar features could control access to data about U.S. citizens. "A lot of the technology we put [in] is to protect rights," says Fuchs.

Like other big-data projects, the NSA team's system, called Accumulo, was built on top of open-source code because "you don't want to have to replicate everything yourself," says Fuchs. But participating in the open-source community wasn't easy. When it came up with improvements, Fuchs's group had to find a third party to suggest a change without mentioning the NSA. That's why the NSA eventually decided to open-source Accumulo as well. Even though the move presented risks (coders' names would be known, and they could become targets of foreign surveillance), the NSA concluded that it would benefit if a wider community of software programmers worked on Accumulo.

In 2011, the NSA released 200,000 lines of code to the Apache Foundation. When Atlas Venture's Lynch read about that, he jumped—here was a technology already developed, proven to work on tens of terabytes of data, and with security features sorely needed by heavily regulated health-care and banking customers. When Fuchs's NSA team got cold feet about leaving, says Lynch, "I said 'Either you do it, or I'll find five kids from MIT to do it and they'll steal your thunder.'"

Eventually, Fuchs and several others left the NSA, and now their company is part of a land grab in big data, where several companies, like Splunk, Palantir, and Cloudera, have quickly become worth a billion dollars or more.

Over the summer, when debate broke out over NSA surveillance of Americans and others, Sqrrl tried to keep a low profile. But since then, it has found that its connection to the $10-billion-a-year spy agency is a boost, says Ely Kahn, Sqrrl's head of business development and a cofounder. "Large companies want enterprise-scale technology. They want the same technology the NSA has," he says.

For some startups, the spying scandal has been good for business. Large companies want the same technology the NSA has.

The Sqrrl team is working 16-hour days. Fuchs says the pace is far more intense than it was at his old government job. But there are things he misses. His top-secret security clearance is on hold, and he's no longer part of the mission to protect the country. For the researchers and developers inside the NSA, "it's hard to empathize with whoever leaves," says Fuchs. "There's no system inside the NSA to leave and start companies. We wanted to maintain contacts, but it's been a challenge."

—Antonio Regalado

Emerged Technologies

For Swiss Data Industry, NSA Leaks Are Good as Gold

Here's how the Swiss promise to keep your data safe.

● There is data security, and then there is Swiss data security.

The difference was explained to me by Stéphan Grouitch in a conference room deep within a mountain in the Swiss Alps, lit by a subterranean buzz of fluorescent lights. To get to here, under more than 3,000 feet of stone and earth, I showed my passport (something I didn't have to do to enter the country from Germany), had my finger scanned repeatedly, and passed under security cameras and motion detectors. A blast door, thicker than my forearm is long, is said to protect this old Cold War bunker against a 20-megaton bomb.

"The country has always stored valuables for people all around Europe—even before money," says Grouitch, CEO of Deltalis, the company that owns the bunker. When Deltalis first looked into acquiring the facility from the Swiss military, it considered storing gold bullion here. Instead, it now runs a farm of computer servers where data is safeguarded by strict privacy laws and a unique culture of discretion. To legally access someone's data here, you'll need an order from a Swiss judge.

A Swiss play in data security has been under way for around a decade, mostly in connection to banking. But the controversy around global surveillance by the U.S. National Security Agency is "a huge development," says Franz Grüter, CEO of Green, an Internet service provider whose state-of-the-art data center in the village of Lupfig is being filled out "years ahead of schedule."

SOURCE: DIRECTOR OF NATIONAL INTELLIGENCE; INCLUDES RELATED DEFENSE PROGRAMS

BE THE ONE WHO MAKES MOBILITY SECURE

Empower business through security.

With a workforce that's truly mobile, you know that protecting everyone's data now extends far beyond the walls of your office. So when your Sales Director leaves for another meeting, it's up to you to ensure their business data is kept safe – wherever it goes.

Kaspersky Security for Business includes mobile device management as part of its easy-to-use security platform.

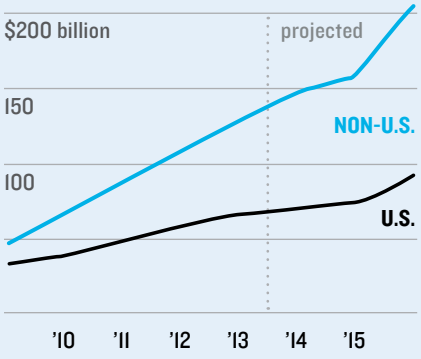
With Kaspersky, you can help the business achieve the gains that mobility can bring, without the security risks.

kaspersky.com/business

#securebiz

KASPERSKY lab

Spread the Risk
Cloud computing spending is shifting away from the U.S.



To get a sense of the opportunity, one need only look at the projected losses the U.S.-based cloud services industry (including Google, Microsoft, and IBM) is facing because of anxiety and indignation over U.S. wiretapping. Estimates of lost market share through 2016 range from $35 billion to $180 billion (according to Forrester Research).

Switzerland isn't the only country hoping to cash in. Finland's F-Secure recently released a Dropbox competitor called Younited. And a consortium of German telecoms, ISPs, and e-mail providers has backed an "E-Mail Made in Germany" program that aims to keep communication data routed and stored in-country when possible. In February, German chancellor Angela Merkel attended talks in Paris on building an all-European communications network so that "one shouldn't have to send e-mails and other information across the Atlantic."

European companies, according to Grüter, now routinely question where data is physically stored—and are declining U.S. offers. One result is that a cluster of privacy companies is forming in Switzerland. ID Quantique makes the Centauris CN8000, one of the world's first commercial encryption systems using quantum mechanics. And Blackphone, a secure handset launched by U.S. privacy pioneer Phil Zimmerman, will store subscribers' telephone numbers in Swiss servers.

Altogether, Switzerland has around 1,440,000 square feet of data-center space. While that is far less than is available in countries like the U.S. and Germany, it's a large amount when compared to Switzerland's population of 8 million.

Richard Straub, head of market development at ID Quantique, says Swiss innovations are backed by strong research at universities like EPFL in Lausanne, ETH-Zürich, and the University of Geneva. They also benefit from local demand. When ID Quantique took its products to market, it found early, and eager, customers in the banking industry and in government. Officials in Geneva have used its technology to help transmit federal election results since 2007, and in online voting for citizen initiatives since 2009.

European companies are now routinely questioning where data is physically stored.

So who can you trust with your data? Grouitch thinks Switzerland's appeal should be obvious. "This country really is a vault in the center of Europe," he says.

—Russ Juskalian

Emerged Technologies

The Year of Encryption

Government spying gives a giant push to cryptography on the Web.

● Last summer, the world's largest Internet companies learned they'd been hacked by the U.S. government.

Their answer for 2014: encrypt everything.

Over the last eight months, Yahoo encrypted its e-mail service and Google extended encryption to every search term that users enter. Microsoft said that by the end of this year it plans to encrypt all the data traveling to and from its networks. "Encryption on the Web is expanding enormously," says Peter Eckersley, technology projects director at the Electronic Frontier Foundation (EFF), which grades companies on how well they do at protecting users' privacy.

The EFF believes that within a few years, every file crossing the Internet could be protected with encryption, which uses mathematics to scramble and unscramble messages.

Encryption does not guarantee complete privacy—ciphers can be broken or compromised. But its widespread use could seriously hinder both cybercriminals and bulk collection of data by governments. That's because even someone who is able to pilfer encrypted data can't easily read it.

Encryption was already a rising trend, even before the spy scandal. Major security breaches have shown that computer networks are not safe from intruders. Last year, hackers stole millions of credit card numbers from Target and Neiman Marcus after finding clever ways to gain access to their systems.

"Today's networks are like Swiss cheese. It's very easy to get in, move laterally, and exfiltrate data," says Dmitri Alperovitch, cofounder of the security firm CrowdStrike. "People are using tools from the 1990s to do it."

Encrypting data, like customers' credit card information, is an additional line of defense. But encrypting stored data (in contrast to data in transit) turns out to pose a difficult puzzle. Encrypting the data protects it but also makes it difficult to search or process—rendering it less useful.

Encryption also takes up computer time, the main reason Web companies like Yahoo didn't always use it before. But Internet firms realize they must now take extraordinary steps in response to extraordinary new threats.

—Robert Lemos

SOURCE: THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Emerged Technologies

For $3,500, a Spy-Resistant Smartphone

Prime ministers, business executives, and ordinary citizens clamor for phones that can't be snooped on.

● Ever since Edward Snowden came forward with a trove of secret documents about the National Security Agency, business has been booming for Les Goldsmith, CEO of ESD America.

Goldsmith's company sells a $3,500 "cryptophone" that scrambles calls so they can't be listened in on. Until recently, the high-priced smartphone was something of a James Bond–style novelty item. But news of extensive U.S. eavesdropping on people including heads of state has sent demand from wary companies and governments soaring. "We're producing 400 a week and can't really keep up," says Goldsmith.

The Las Vegas–based company prepares and packages the device, called the GSMK CryptoPhone, by first wiping the software from an ordinary $350 Samsung Galaxy S3 handset. It then adds a version of Google's Android operating system, licensed from the German company GSMK, that's has been tweaked to add call encryption and fix security flaws.

Sales have tripled since Snowden's revelations began last June, and close to 100,000 of the handsets are in use worldwide, according to Goldsmith. Secure calls work only between two cryptophones. To set up a secure connection, each handset creates a cryptographic key based on a sample of random background noise. Everything takes place on the handsets, so no unprotected data leaves the device.

Secure phones aren't new. In the 1970s, the NSA developed a "secure telephone unit" that featured an ordinary-looking push-button landline phone connected to a crate-size scrambler. What has changed is that consumer smartphones have created an explosion of new opportunities for snooping. Handsets can be infected by malware that listens to calls, copies data, or transmits a device's location. Some spies even employ fake base stations, known as interceptors, that harvest calls and text messages.

That's reason enough for politicians, dissidents, and top executives to worry. Last year, the prime minister of Turkey ordered cryptophones for all his ministers after discovering bugs in his office and car. At ESD, Goldsmith says, most of his customers are U.S. multinationals worried about economic espionage by China, whose military conducts large-scale efforts to pilfer data. "We get a lot of people who have had information from one-to-one discussions over the telephone somehow get out," he says.

Examples aren't hard to come by. In February, a politically embarrassing conversation between a U.S. State Department staffer and the American ambassador to Ukraine was leaked onto YouTube. "All Department of State government-owned BlackBerry devices have data encryption. However, they don't have voice encryption," said State Department spokeswoman Jen Psaki.

The CryptoPhone's $3,500 price tag includes three years of service, not including calling charges. That puts the device beyond the reach of most individuals and small businesses. A competing device, the Hoox m2 smartphone that French IT contractor Bull began selling in January, sells for 2,000 euros ($2,740) and is also aimed at corporate users.

For the most part, consumers haven't joined the security rush. According to Gartner, a firm that tracks technology trends, few have even purchased antivirus software for their phones. Sales of mobile security software are about $1 billion a year, a fraction what's spent on desktops, even though mobile devices now outnumber PCs.

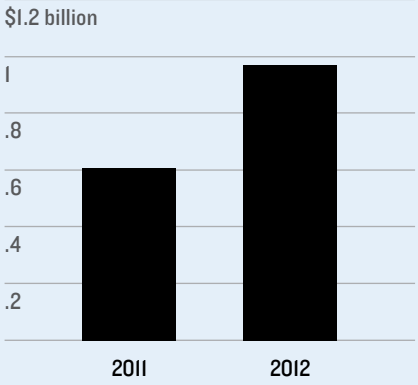
Yet secure communication products could eventually have mass appeal as consumers tire of being tracked online. Some of the most successful apps of the past year have featured self-destructing messages or anonymous bulletin boards.

Companies on a budget could turn to the $629 Blackphone handset, which launched in February and also offers encrypted calling. The device is the product of a joint venture between Spanish smartphone startup Geeksphone and Silent Circle, a company that markets apps for encrypted calling and e-mail on Apple and Android devices.

The Blackphone lacks some premium security features, like the ability to foil fake-base-station attacks, and it isn't marketed as being "NSA-proof" either. But it still offers significantly better security and privacy than a conventional handset, says Javier Agüera, cofounder and chief technology officer of Geeksphone. "Blackphone is for the people, not just a small elite," he says. —*Tom Simonite*

Run to Safety

Global spending on security software for mobiles is growing



SOURCE: MIT TECHNOLOGY REVIEW | SOURCE: INFONETICS

Cryptophones Offer Secure Calls

Blackphone	$629	Disables Wi-Fi tracking
GSMK CryptoPhone	$3,500	Secure Samsung Galaxy S3
HOOX m2	$2,740	Biometric identification
In Confidence	$1,659	Unlimited Internet calls
Secusmart	$3,436	Encrypted BlackBerry Z10

Industry Guide

Computer Security

The key executives, technology startups, and industry resources you'll need in order to understand how government espionage is changing the technology businesses.

EXECUTIVES TO WATCH

Keith Alexander

Director, National Security Agency
Fort Meade, Maryland

West Point graduate Keith Alexander may hold the most important IT job in the world: overseeing a $10 billion global spying and cyberdefense operation that employs some 30,000 people. He has led the NSA, America's key signals intelligence agency, since 2005. Insiders applaud Alexander for taking transformative steps, including moving the agency toward modern cloud computing and erecting a vast data center in Utah. Yet Alexander's term also saw the biggest intelligence leak in history, one that revealed many details of the NSA's broad surveillance activities, including its collection of Americans' phone records. Alexander is expected to depart the agency in 2014.

COMPANIES TO WATCH

CipherCloud

Cloud encryption
San Jose, California
Founded: 2010
Raised: $31 million
Investors: Andreessen Horowitz, Index Ventures, T-Venture

Venture capitalists once viewed computer security as boring, a solved problem. Not anymore. They have been racing to invest in security startups, putting nearly $1.4 billion into some 200 companies during 2012. CipherCloud's motto is "trust in the cloud." The problem is that large companies want to store transaction data, including credit card numbers, in cloud services—but it's not safe enough. Encrypting the data can secure it but also makes it inaccessible to apps and limits its usefulness. CipherCloud says it has found a way to use representations of stored data to make it both secure and searchable. As data moves to the cloud, encryption is expected to follow. Cofounder and CEO Pravin Kothari says the cloud is the "biggest killer application for encryption" since e-commerce a decade ago. "Most companies don't anyone looking at their data," he says. "And that includes the government."

EXECUTIVES TO WATCH

Arthur Coviello

Executive Vice President, RSA
Hopkinton, Maryland

Arthur Coviello is in the hot seat. His company, RSA, sells computer security products—and that makes it everyone's target. In 2011, RSA's SecureID token system for logging into laptops was hacked, leading to intrusions at companies like Lockheed Martin. Coviello reacted with a detailed public investigation. Reputation restored. But then, in 2013, leaked government documents showed that RSA's key cryptography software, BSafe, had been intentionally weakened by the U.S. National Security Agency (which had also paid RSA $10 million). This time around, RSA has offered only vague explanations, exposing it to wide criticism among security experts, cryptographers, and its own staff. During RSA's annual conference in 2014, Coviello sought to shift the blame for the fiasco to the NSA, saying, "When [the government] exploits a position of trust, that's a problem."

COMPANIES TO WATCH

CrowdStrike

Identifying advanced persistent threats
Irvine, California
Founded: 2011
Raised: $56 million
Investors: Warburg Pincus, Accel Partners

CrowdStrike is one of an emerging wave of companies that specialize in iden-

Who to Follow

Dmitri Alperovitch
CTO, CrowdStrike
@DmitriCyber

Jeffrey Carr
Founder, Suits and Spooks Conference, Taia Global
@jeffreycarr

Tom Field
Editorial Director, Information Security Media Group
@SecurityEditor

FireEye
Security Company
@fireeye

the grugq
Hacker
@thegrugq

Mikko Hypponen
Chief Research Officer, F-Secure
@mikko

Eugene Kaspersky
CEO, Kaspersky Lab
@e_kaspersky

Brian Krebs
Investigative Journalist, Krebs on Security
@briankrebs

U.S. National Security Agency
Job Board
@NSACareers

Andrea Peterson
Cybersecurity Reporter, Washington Post
@kansasalps

Bruce Schneier
Security Technologist and Author, Co3 Systems
@schneierblog

Christopher Soghoian
Principal Technologist, ACLU
@csoghoian

Aliya Sternstein
Senior Correspondent, Nextgov.com
@Aliya_NextGov

Women in Security
Advocacy Group
@WomeninSecurity

BE THE ONE WHO PROTECTS THE BUSINESS

Empower business through security.

You can't keep an eye on everyone. Often, people are the weakest link, even when they're working their hardest. From visiting inappropriate websites to accidently downloading a virus, business can be interrupted – and you know it's your job to get everything back on track, fast.

Kaspersky Security for Business brings together powerful anti-malware and control tools, encryption, mobile and systems management into a single integrated platform.

Empower your colleagues to work the way they want to, without the security risks.

kaspersky.com/business

#securebiz

KASPERSKY lab

tifying state-sponsored cyberattacks, known as "advanced persistent threats." The company profiles attackers using a big-data approach to identify intrusions. It monitors company networks and studies signatures of malware and other factors to understand threats. The company also gathers intelligence about possible motives for an attack. CrowdStrike founder Dmitri Alperovitch says the threat from nation-states is expanding. While threats from China are widely appreciated, his firm is now tracking attackers from Iran that have targeted the financial sector, as well as new cyber-offensives from Pakistan, North Korea, and the Russian Federation. "More and more advanced and developed countries are getting involved," says Alperovitch.

COMPANIES TO WATCH

Endgame

Offensive computer security
Arlington, Virginia
Founded: 2008
Raised: $56 million
Investors: Bessemer Venture Partners, Columbia Capital, Kleiner Perkins Caufield & Byers

Forbes magazine has called Endgame "the Blackwater of hacking." For good reason. The company was until recently part of a small, extremely controversial industry that creates "zero-day" exploits, or entirely new ways to hack into computers. Endgame sold these exploits to U.S. intelligence agencies for prices said to reach millions of dollars. The industry, tightly intertwined with governments, includes Vupen Security in France, Hacking Team in Italy, and Gamma Group in the U.K. These companies have become increasingly open about what they do—even advertising their services on the Web. But Endgame is also growing up. Its 36-year-old CEO, Nate Fick, a former Marine, says he has gotten Endgame out of the questionable "zero-day" business and is turning it into a top-tier security firm, specializing in big-data analysis and vulnerability intelligence.

COMPANIES TO WATCH

Microsoft

World's leading PC operating system
Redmond, Washington
Founded: 1975
Vital statistics: $77 billion in sales and 99,139 employees

By some measures, Microsoft is the world's largest computer security company. Its operating system, Windows, is on most PCs. That also makes it a frequent target of attacks by cybercriminals. In a significant shift, Microsoft has decided to go on the offensive, and last year it pushed ahead with what it calls "active response." It began paying for vulnerabilities in its software, handing out bounties as high as $100,000, to take them out of the market. Then in December, Microsoft's Digital Crimes Unit collaborated with the FBI and Europol to attack and disable a network of two million infected computers programmed to commit click fraud on search ads. The company's assault on the botnet, called ZeroAccess, aimed to inflict economic damage. On exactly who, it's not clear. The botnet's authors were not identified.

EXECUTIVES TO WATCH

Kevin Mandia

SVP & COO, FireEye
Milpitas, California

A computer scientist, forensic expert, and former Air Force officer, Kevin Mandia founded the computer security firm Mandiant and then sold it to the security software provider FireEye in a deal worth over $1 billion in January 2014. His company had become well known after publishing details of Chinese espionage and theft of intellectual property, tracing the attacks to a Shanghai office building run by the Chinese army. His firm specialized in "digital forensics," or cleaning up after companies get hit by cyberattacks—a growing business. The price paid for his consulting firm reflects a red-hot market for security services and products focused on "advanced persistent threats" such as Chinese espionage.

Where We Are Going

United States Cyber Crime Conference
April 27–28, 2014
National Conference Center
Washington, D.C.
www.usacybercrime.com

Gartner Security & Risk Management Summit
June 23–26, 2014
Gaylord National
National Harbor, Maryland
www.gartner.com/technology/summits/na/security

Cyber Defense Initiative Conference
July 30–31, 2014
Bangkok International Trade & Exhibition Centre
Bangkok, Thailand
www.cdicconference.com

RSA Conference Asia Pacific & Japan
July 22–23, 2014
Marina Bay Sands
Singapore
www.rsaconference.com/events/ap14

Black Hat
August 2–7, 2014
Mandalay Bay
Las Vegas, Nevada
www.blackhat.com

Crypto 2014
August 17–21, 2014
University of California, Santa Barbara
Santa Barbara, California
www.iacr.org/conferences/crypto2014

ICETE 2014 11th International Joint Conference on E-Business and Telecommunications
August 28–30, 2014
Vienna, Austria
www.secrypt.icete.org

Computers, Privacy & Data Protection 2015
January 21–23, 2015
Les Halles de Schaerbeek
Brussels, Belgium
www.cpdpconferences.org

RSA Conference 2015
April 20–24, 2015
Moscone Center
San Francisco
www.rsaconference.com

BE THE ONE WHO PUTS SECURITY ON THE AGENDA

Empower business through security.

Another Friday, another senior management meeting. You know that future business will require more IT projects for you to manage, but is anyone discussing security? It's your job to ensure they do.

Kaspersky Security for Business is the world's first integrated security platform. It enables your business to take advantage of mobile device management, encryption and systems management, as well as having Kaspersky's award-winning anti-malware protect your organization.

You can put security on the agenda with Kaspersky.

kaspersky.com/business

#securebiz

KASPERSKY lab

What We Are Reading

REPORTS

The Next Wave, The National Security Agency's Review of Emerging Technologies
U.S. National Security Agency
Marion J. Roche
The Next Wave is the bulletin of the National Security Agency's technology transfer program, which forms collaborative R&D agreements with industry and licenses agency inventions in optics, semiconductors, and semantic analysis software. The bulletin provides an unexpected look inside a leading spy agency, whose more than 1,000 mathematicians, 960 PhDs, and 4,000 computer programmers are responsible for over 170 patented inventions.

Report on the Telephone Records Program
Privacy and Civil Liberties Oversight Board, January 2014
David Medine et al.
This 238-page report is an exhaustive look at the history and legality of the National Security Agency's bulk collection of American telephone records under Section 215 of the USA Patriot Act. Under the program, companies like Verizon handed over basic records of every call made in the U.S. The federal oversight committee concluded in a 3-2 vote that the program is illegal.

Foreign Spies Stealing US Economic Secrets in Cyberspace
Office of the National Counterintelligence Executive, October 2011
The most recent in an annual series of federal reports describing the known risks to U.S. companies of foreign economic and industrial espionage in cyberspace, focusing primarily on the activities of the governments of China and Russia. The report data was assembled with the assistance of 26 agencies and 21 private-sector organizations.

APT1: Exposing One of China's Cyber Espionage Units
Mandiant, February 2013
Kevin Mandia et al.
It's not news that China's People's Liberation Army conducts cyber-espionage. But this 74-page report made headlines by offering unprecedented detail on the operations of a Shanghai-based military unit intent on stealing company secrets and spying on political opponents in the U.S. and elsewhere. The report illuminates how investigators piece together digital clues to draw a disturbing picture of a rising threat.

BOOKS

Liars & Outliers
Wiley, 2012
Bruce Schneier
When the U.S. Congress needed to understand what its own spy agencies had done, they called security expert Bruce Schneier. In *Liars & Outliers*, Schneier cuts beyond technical questions to the foundational issue of security—the question of trust. He discusses the social and biological underpinnings of trust, the importance of trust to society and business, and the changing nature of trust in the information society.

Sinophobia: The Huawei Story
Amazon Digital Services, 2013
Eric C. Anderson
In this self-published e-book, Eric Anderson, a faculty member with the National Intelligence University, traces American fears of China from the gold rush to the cyber age, providing dense detail on how world's largest telecommunications equipment company became—fairly and unfairly—the focus of U.S. cyber-espionage fears.

The Shadow Factory
Anchor, 2009
James Bamford
Before the Snowden leaks, so little was known about the ultrasecret U.S. National Security Agency that it was called "No Such Agency." In this book, a follow-on to his 1983 *The Puzzle Palace*, James Bamford explains how after missing warning signs of the 9/11 attacks, U.S. eavesdroppers set out to collect vastly increasing amounts of digital data, including data on Americans. For anyone interested in the politics of spying and of running huge government agencies, Bamford's book is necessary background.

EXECUTIVES TO WATCH

Christopher Soghoian

Principal Technologist, ACLU Speech, Privacy and Technology Project
Washington, D.C.

Christopher Soghoian has been on a tear against bad privacy practices online, urging companies to change the way they operate—and sounding the alarm if they don't. The security researcher helped develop the Do Not Track mechanism that lets people prevent websites from following their online activity, pressured Google to encrypt its Gmail service, and served as the first in-house technologist at the Federal Trade Commission. He says his goal is to make sure "everyone has secure communication." Since joining the ACLU in 2012, he has continued to raise alarms about how easily law enforcement and criminals can delve into our growing storehouses of personal data.

EXECUTIVES TO WATCH

Phil Zimmermann

Cofounder, Silent Circle
National Harbor, Maryland

Phil Zimmermann has been trying to make encryption mainstream since the 1980s, when he came up with PGP, an encryption algorithm meant to protect citizens against government surveillance. After his source code was published on the Internet in 1991, U.S. prosecutors opened a criminal investigation over whether this violated export controls; the probe was eventually dropped. But his technology remained popular. Now a company he cofounded in 2012, Silent Circle, sells subscriptions to secure voice and text communications using newer versions of PGP. Its latest offering is a secure phone, known as Blackphone, that tries to embody these ideals in a piece of consumer hardware.

COMPANIES TO WATCH

Virtru

Secure e-mail
Washington, D.C.
Founded: 2012
Raised: $4.2 million
Investors: Angel investors

Virtru is developing what it calls a "secure zip file" that can wrap around any type of data, irrespective of format. The startup and its technology (called Trusted Data Format) is notable for originating inside the U.S. National Security Agency, where founder Will Ackerly and seven other Virtru engineers once worked as programmers. Virtru believes it is the only NSA spinoff company developing products aimed at the consumer market. The company says its goal is "giving the everyday consumer back control of their private information," particularly e-mails and attachments.