TECH 40 UNDER 40

Could this ex-NSA hotshot protect your email from hacking?

BY

LUKE O'BRIEN

September 24, 2015 11:00 AM EDT

One morning in June 2013, Will Ackerly opened his laptop in his Washington, D.C., apartment and began to worry. The *Guardian* had just published the first of its bombshell articles about the National Security Agency's secret bulk collection of Americans' personal data. Someone was leaking secrets.

Am I going to get a phone call? Ackerly wondered, downing a five-shot espresso.

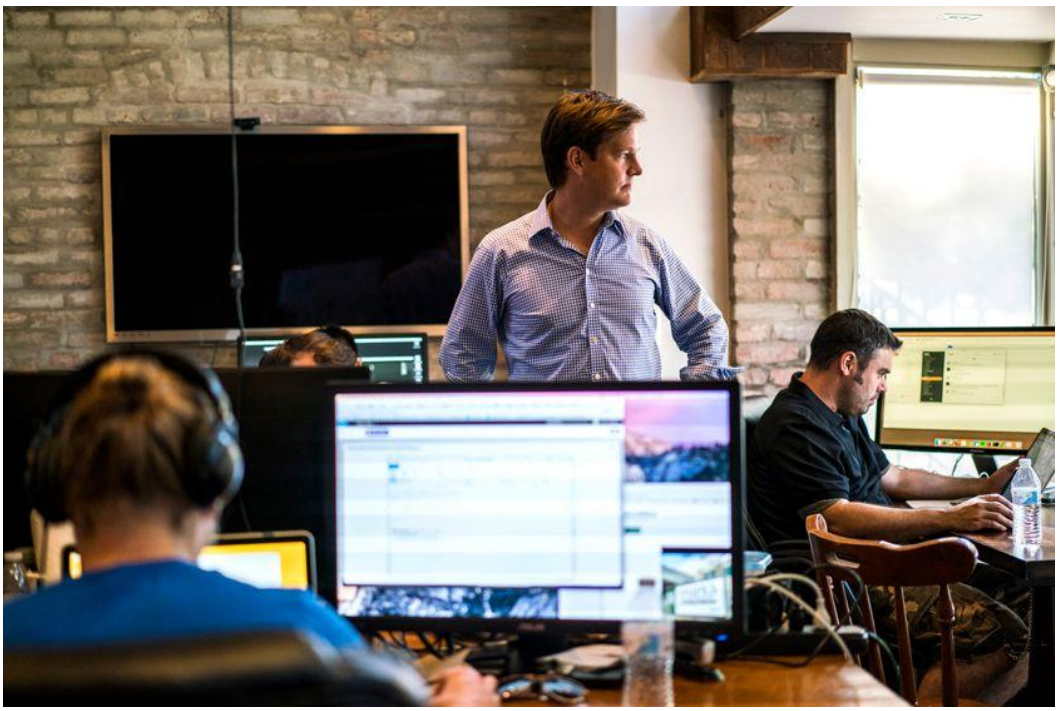
It wasn't an unreasonable question. Less than a year earlier Ackerly had left his job at NSA headquarters in Fort Meade, Md., where he had worked as a lead security architect for the agency's first cross-domain cloud, a vast database that could connect information on almost anything about anyone. Ackerly had been exposed to a wide range of NSA programs. He'd designed futuristic gadgets and computer systems and been deployed to Iraq to help capture a master bombmaker. All that was in his file. What wasn't: He'd recently driven to the Rhode Island seashore with his girlfriend, who was running a Booz Allen Hamilton encryption team, and asked her to marry him. Two of their friends were there; one happened to work for the *Guardian.*

This coincidence, Ackerly knew, was exactly the kind of data point the NSA tracks from the digital shadows. He'd witnessed the agency's dragnets, which suck in trillions of texts, call

logs, and pieces of email metadata, and the court rulings that, in his view, overrode civil liberties. “If you are in their sights on an individualized basis, it’s ‘game over,’ ” Ackerly says. Now he had an inkling of what it felt like on the wrong side of the lens.

A few days later, to Ackerly’s relief, Edward Snowden came forward as the *Guardian*’s source. What followed was a deluge of classified documents that revealed what a leviathan the NSA had become after 9/11. Like Snowden, Ackerly found the agency’s rampant power alarming. Unlike Snowden, he says, he was never going to leak.

Ackerly knew he couldn’t prevent mass surveillance—but he could at least try to shield people’s information. So he founded a company, Virtru, based on a technology he invented to sheathe individual pieces of data with encryption. He called his creation the Trusted Data Format, or TDF. It makes it dramatically harder for anyone—a private hacker, a foreign state, or one’s own government—to pilfer what users want to protect.



John Ackerly, a former private equity executive, pictured at Virtru’s offices. He runs the business while his brother focuses on technology. Photograph by Benjamin Lowy for Fortune Magazine

Ackerly launched his business with several former NSA colleagues and his brother John, who had worked on tech policy in the George W. Bush administration. (Disclosure: I knew John Ackerly in high school.) To Will Ackerly, the most obvious application for the TDF was email. Nobody had figured out a way to encrypt email that was simple enough for universal use. Ackerly believed he could. He didn't just want to help companies defend against data breaches. He hoped to give everyday Internet users a way to protect themselves online.

The Snowden leaks lent momentum to Ackerly's mission, which has only intensified as disastrous hacks have penetrated institutions ranging from the federal government to Sony Pictures (SNE), Anthem, J.P. Morgan Chase (JPM), Target (TGT), and even Ashley Madison. Data security has become more crucial than ever for individuals, corporations, and governments.

Thousands of companies have embraced Ackerly's technology, including Google (GOOG), which has partnered with Virtru to serve enterprise customers. Outside observers are also impressed. "I think Virtru will have a great impact on the health care space," says Trung Do, executive director for business development at Partners HealthCare, the parent of several New England hospitals, including Massachusetts General. "They have a pretty ubiquitous platform that's easy to use and is cheap. This thing can scale. That's futuristic to me."

Ackerly himself doesn't quite fit the traditional picture of the business virtuoso who makes *Fortune*'s 40 Under 40 list (No. 21). He's an idealist as much as an entrepreneur, one who believes that the best way to transmit his ideas is through a company. His brother, CEO of Virtru, is the real businessman in the family. The fledgling company is miles away from an IPO; for now Will Ackerly is paying himself about $30,000 a year and supplementing that salary with poker winnings. What's most important to Ackerly is his earnest dream: that millions of people will use his technology to protect their privacy.

Should Ackerly's TDF attain widespread use, it will mean a technology invented by an NSA staffer with the original goal of helping the intelligence community protect its own information may end up as a tool to block the government's mass data grabs. It's among the many paradoxes of the cyber arms race. Here's another one: Businesses pay billions each year for network security. Essentially, they put a firewall around a data cache and pray. But Ackerly and others argue that it's far more effective to safeguard each piece of information, as the TDF does. This "data-centric" approach is becoming a new cybersecurity paradigm, and Virtru is in a perfect position to capitalize on it.

Will Ackerly, who turns 35 on Oct. 2, has the frame of a heavyweight rower and a large head that bobs when he gets excited, which is often. When we met at the Hans Pedr' Kaffe in Washington this past January, he held forth on multiple technical matters, peppering the discussions with dry wit. He described a theory for putting vehicles into orbit without rockets by shooting lasers at photovoltaic panels, then segued into a deadpan *Austin Powers* riff about attaching lasers to sharks. Among the things that excite him are the *Simpsons,* problems to be addressed and solved, and cooking new dishes with his wife. Ackerly's enthusiasm is such that, at one point, occupants of a nearby table glanced over.

Will Ackerly Photograph by Benjamin Lowy for Fortune Magazine

The mysteries of code and cognition hold a special appeal. At high levels, mathematical theory and computer science can bleed into what feels like philosophy, and Ackerly can ramble on in this vein. A single question can produce a four-hour answer ranging across satellite artwork, quant trading, and how snobby the CIA can be. He has always had a roving, intense curiosity.

A question about voice-recognition technology elicited cryptic allusions from Ackerly about “some institutions that would be particularly motivated to be the best in the world when it comes to hearing multiple voices and understanding what they’re saying.” Then he was off on a tangent about the neocortex of a deaf and blind ferret. Before I knew it, he was talking

about using the neocortex—of a human—to find patterns and pull signals out of noise from audio and stock market data. A lot of it had to do with the “expectation flow” of inputs such as images that could be propagated through the brain and create a “difference engine” to detect anomalies. “That whole area fascinates me,” he says. “I’d love to get into it.” Ackerly is precisely what you would imagine an NSA whiz kid to be.

The letter from the NSA arrived in the fall of 2003. It contained instructions out of a bad spy movie: *Call this number. Arrive at this hotel. Speak this code word to the receptionist.* A few days before, Ackerly had been sitting in class at the Rose-Hulman Institute of Technology in Terre Haute, Ind., finishing up a dual degree in electrical and computer engineering. He had sent in his résumé over the summer. Now he had landed an interview. He had no idea what the job was. But he followed instructions and booked a flight to the Baltimore-Washington airport. When he got there, a van took him to a nearby hotel, where Ackerly approached the receptionist with his code word, an acronym for a made-up organization.

“Hi,” he said, trying to act nonchalant. “I’m with OHA.” The receptionist flashed him a knowing smile. “Someone will be coming shortly.”

Within minutes a taciturn middle-aged man in khakis and a windbreaker materialized. He checked Ackerly’s identification and ushered him into a different van, with northrop grumman on the side. The man barely spoke as they headed for Fort Meade, the nerve center of the “No Such Agency,” where cellphone signals drop off the grid and other taciturn men materialize on the shoulders of roads to change flat tires for motorists to keep them moving. (The NSA declined any comment for this article.)

As the van neared the fort, it maneuvered slowly through zigzag barricades and checkpoints manned by the NSA’s heavily armed, black-clad paramilitary police. Several of them sat behind sandbag emplacements with SAW machine guns. Looming above it all

were the OPS2A and OPS2B buildings, ominous black monoliths girded underneath in copper Faraday cages to block electromagnetic waves. Reflective, bulletproof windows made from tinted double panes of copper-laced glass prevent signals from leaking out. Classical music plays between the panes to further stymie eavesdroppers. Ackerly couldn't wait to get inside.

The OPS2A and OPS2B buildings at NSA'S headquarters in Fort Meade, MD. Their exterior glass is laced with copper to prevent signals from leaking; classical music plays to deter eavesdropping. Getty Images

The NSA is said to employ more mathematicians than any organization in the country. Some 1,000 work there, according to recent media reports, along with some 4,000

computer programmers. Ackerly had the ideal background to join them. Growing up in a well-heeled family in Washington, D.C., he'd shown a mischievous, quirky intelligence from early on. He built train sets with his dad, who taught him basic electronics, and played with Capsela, a construction toy with gears and motors. But he generally had more fun taking toys apart to see how they worked. When he was 5 his parents gave him a chemistry set, which led to several fires in the house.

Around the same time the family bought its first computer, an Apple IIGS (AAPL). "Watching a computer be set up and get turned on for the first time was just an amazing sequence of events," Ackerly says. "I was hooked." He wrote his first program, a simple car-racing game, when he was 7. By 10 he'd learned BASIC from an older computer whiz at school. The two would connect by modem to play games and code. To conceal his excessive modem use, Ackerly rewired a switch in the basement to disable a light on his parents' phone system. In eighth grade he was nabbed hacking into his school's computer system. "I got bored," he says. That was typical in high school, too, where he rarely felt challenged in math and science and neglected his homework. His grades suffered, even as he excelled on elite national tests, such as the American Invitational Mathematics Exam. Learning from textbooks didn't interest him the way puttering around with electronics and code did. At heart he was a tinkerer.

Now he was walking into an organization that tinkered on an unprecedented scale. An NSA scientist showed him racks of equipment to test high-speed photonic communications and walked him past computers that created virtual networks. Within those networks a user could use simulated computers to form other networks, creating a nesting doll of secure workspaces. "What we're trying to do is make the very best encryption work faster," the scientist told him.

Ackerly left the interview in a daze. A few months later another letter arrived. Pending a background check, the NSA had a position for him. The salary was $47,000. He'd start work

the coming summer. He still didn't know what the job was. But he knew he couldn't pass it up.

In August 2004 he joined the information assurance arm of the NSA's research directorate. Protecting data—Ackerly's initial role—gets less glory, but it's just as important as hacking. His colleagues were odd and brilliant. (An old joke at the agency captures the stereotype: "How can you tell an extrovert from an introvert at the NSA?" Punch line: "The extrovert stares at *your* shoes."). Ackerly could relate. He could concentrate intensely—he would win big playing round-the-clock poker—but his brain would also "jump" and free-associate to make unusual connections.

Ackerly's job was to create hardware and software to protect information. He experimented with swapping a computer's normal identity chip for ones that allowed the machine to safeguard top-secret info. He built a tamper-resistant USB log-in fob that would self-destruct if an adversary tried to get in. "It felt like we were building the future," he says.

Of all his projects, secure virtual networks excited him the most. Such networks let groups of users connect to a protected enclave of data to collaborate. They met a pressing need within the intelligence community: Stovepipe databases couldn't communicate with one another, and the future was about sharing. The government was shifting from a "need to know" mind-set, which segregated data by agency and mission—a stance seen as one culprit in the failure to prevent the 9/11 attacks—to a "need to share" approach that emphasized data fusion. The idea was to connect as many dots as possible and prevent another attack.

But secure virtual networks have a weakness. Users can't connect dots across networks with different levels of classification and access policies. On a joint task force, FBI agents might not be able to access the same material as CIA analysts or NSA linguists. For every group working together, you needed to create a new network and import the data.

Ackerly saw a possibility: Eventually networks would become so specialized that they would shrink until they surrounded only one dot—a single piece of data—like a shell. When that happened, you were no longer securing the location of the data. You were protecting the data itself, which allowed it to safely move anywhere. The barriers to collaboration disappeared. Here was the first insight that would lead him to his data wrapper.

Ackerly worked at the NSA during a period in which the agency's reach vastly expanded. In the aftermath of 9/11, it was a time of war and the NSA had been unleashed not only abroad but also at home, with Congress and the courts blessing a broad expansion of domestic surveillance.

The extent of the agency's practices only dawned on Ackerly in March 2008, when he attended a presentation by an NSA lawyer at Fort Meade. In four years at the agency, he had never heard anyone lay out the case for the NSA's sweeping powers in that way. As Ackerly understood the explanation, war powers could supercede laws that constrained surveillance. At one point, the lawyer asked for questions. Ackerly stuck up his hand. "Can you think of an example where a domestic surveillance activity would not be granted by war powers?" he recalls asking. The lawyer said he couldn't.

"That's the first time it hit me," Ackerly says now, "where I got a visceral sense that, whoa, something might be really out of whack."

Ackerly's colleagues took privacy seriously, but the attitude at the top disturbed him. By this point he had joined the Systems and Network Interdisciplinary Program (SNIP), a select three-year course in network, hardware, and software protection and the dark arts of hacking and exploitation. Even as Ackerly trained in offensive operations, he kept pondering how to protect data. He believed strong privacy protections needed to be embedded in technology built for the intelligence community.

In February 2009 he had a breakthrough. Ackerly was driving home through a snowstorm when his brain revved up so abruptly that he had to pull into a supermarket parking lot to make sense of his thoughts. Wrapping data with powerful encryption was easy, he knew. The technology existed to do it. Data could also be tagged with controls to restrict who saw it and where it wound up. These tags were part of the metadata around the data, much like the to and from addresses on an envelope around a letter. What Ackerly had dreamed up was a way to lock the envelope (metadata) to the encrypted letter (data) and let the user digitally notarize it. Encrypted data could be moved around safely. Notarized data could be trusted.

Back in the office a few days later, Ackerly sketched out his idea for the Trusted Data Format for a gifted coder colleague. He wanted help building it. His friend didn't hesitate. He thought it was the kind of technology that could drive radical change.

First, though, Ackerly had to go to war.

The Chinook helicopter swooped low over the plains outside Baghdad, its rotors churning the night air. Through the open ramp at the back, Ackerly watched the landscape rush past in the moonlight. A tail gunner, strapped in with a cable, leaned out the ramp as the helicopter banked toward its rendezvous point. Ackerly had geared up with body armor, an M4 carbine, and night vision. He was going after a terrorist and master bombmaker believed to be aiding the Iraqi insurgency.

As part of SNIP, Ackerly had volunteered to deploy to Iraq with the NSA's elite hacker team. The military sorely needed technicians; one in his special operations unit had recently been killed in action. Ackerly learned to shoot, jam signals, and use tracking beacons. When he arrived in Iraq in October 2009 at a base that came under daily mortar fire, his commander set him up with a desk, a soldering iron, and whatever spare parts that could be wrangled. Ackerly reverse-engineered IEDs, hacked vehicle smart keys, and hid antennas inside fake

objects he built with rubber molds. “He was the go-to guy for anything that ran on batteries or plugged into a wall,” says Matt Bach, a Navy technician who worked with Ackerly.

The special ops guys dubbed Ackerly “Q” because of his talent for gadgetry and the strange half-finished devices they found strewn across his desk. Bach took to calling him “Will-bot” because he considered his friend half-man, half-robot. The two spent a lot of time together in the workshop and the gym. Lifting weights was a new hobby for Ackerly; there wasn’t much else to do in Iraq. “Eating, sleeping, and going to the gym,” Ackerly says. “And then playing mad scientist.”

In Iraq, Ackerly learned to shoot and jam signals. The special ops guys dubbed him “Q” because of his talent for gadgetry.

Somewhere near Baghdad the Chinook touched down in hostile terrain. Time to play mad scientist. The helicopter was on the ground just long enough to get a white sedan up its ramp and into its belly. The car belonged to the targeted terrorist. The unit didn’t want to take him down yet. They wanted to monitor him first. Ackerly needed to find a way to track the sedan. He had only a few hours before the target would notice his car was missing.

Ackerly went to work. He can’t reveal the specifics of his methods because they’re classified, but he rigged the car to be easily monitored. In a similar situation later, he used what he had learned to devise an ingenious unclassified technique. In Iraq white sedans are ubiquitous. Thermal cameras on American drones and planes often lost them behind buildings or in traffic. But what if the vehicle had a unique thermal signature? In a desert country, a car’s most useless feature is its rear defroster. Nobody would notice if it wasn’t working properly. Using a knife and a screwdriver, Ackerly came up with a simple way to rewire a defroster to surreptitiously activate when the car’s engine was running and throw a single bold line of heat across the rear window.

For the next 72 hours American forces followed the sedan before snatching the terrorist one night. The mission was a resounding success, and afterward an Army general told Ackerly he could have any job he wanted. Few NSA operatives return to a cubicle after getting a taste of action, but Ackerly couldn't stop thinking about his TDF. He'd seen the military struggle to encrypt communications in the field, where commanders often used open lines because crypto was too complicated or took too long. It was the same for civilians. Solving this problem was more exciting to him than catching bad guys.

Even in Iraq, Ackerly kept thinking about protecting data.

When Ackerly returned to the NSA in March 2010 he became a lead security architect for Accumulo, a cloud-based database whose size was restricted only by the amount of money and bandwidth available to run it. Accumulo could handle the full spectrum of inputs: audio, video, photos, text. You could drop anything into the system—license-plate-tracking data or DNA records—and it would scrape information and allow users to visualize connections across categories. "The number of actual pieces of data—it's incredible," Ackerly says.

His reservations about mass surveillance had deepened. One night he was talking to two mathematicians on the Accumulo team when the subject of classified court rulings came up. These rulings can grant legal powers that let the government clandestinely collect data about people, including Americans. Section 215 of the Patriot Act, for example, allowed the government to acquire "any tangible things" related to a terrorism investigation. The Foreign Intelligence Surveillance Court determined that to mean the phone records of virtually every person in the U.S.

This interpretation was classified. Ackerly was appalled. How could Americans decide what they were okay with if they couldn't even know it was happening? "It was no longer an issue of 'Can we have this [information] or not?' " he says. "The wolf is in the henhouse, and you've got to make sure that the wolf is extraordinarily contained. You can't just put a fence around the henhouse."

Ackerly at the Lincoln Memorial. "the wolf is in the henhouse," he says of government surveillance, "and you've got to make sure the wolf is extraordinarily contained." Photograph by Benjamin Lowy for Fortune Magazine

Ackerly knew his TDF could help. Wrapping each piece of data with encryption would ensure that information could be used only as intended. Ackerly finished a prototype in June 2009 and managed to include it in a small pilot program throughout the intelligence community. The Office of the Director of National Intelligence later adopted it as an official

specification and published it as an open standard, which meant anybody could use the technology.

Inside the NSA, though, Ackerly's technology languished. It was implemented on a limited basis, but his attempts to get it deployed by the organization bogged down in bureaucratic inertia. Ackerly was frustrated. He felt the future he was building might die on a shelf.

He had recruited several colleagues eager to tackle email encryption and settled on a business name that reflected his feelings about privacy: Virtru. It was time to try his luck on the outside. In August 2012, Ackerly dropped his identity badge in a hopper and drove away from Fort Meade and the hidden, fantastic realm that had been his home for eight years.

The federal government has historically fought the democratization of encryption. In the 1970s, for example, the NSA forced the U.S. Patent Office to classify certain inventions for national security reasons. But cryptographers wouldn't be deterred, especially as personal computers became commonplace.

Early attempts at email encryption fizzled because they required both sender and recipient to use a special program, and not enough people did. In the 1990s a computer scientist named Phil Zimmerman created PGP, which could run on different platforms and was circulated throughout the world over the rapidly expanding Internet. The U.S. government responded by investigating Zimmerman for "exporting a munition" but couldn't contain his invention, which allows for end-to-end encryption where only the parties communicating can decipher messages. They do this by exchanging cryptographic keys, which are long, virtually unhackable strings of numbers. It was email encryption for the people—provided the people were techies. PGP would never go mainstream because it was too difficult to use.

Since then, a smattering of services has tried to simplify privacy technology with varying success. Cryptocat is a browser extension for online chatting that Snowden and journalist Glenn Greenwald used. Silent Circle, launched in 2012 by Zimmerman and a former Navy SEAL, provides robust security for phone calls, texts, and videochat, and has found a home among politicians, celebrities, and other VIPs willing to pay to change devices or software. Wickr is an instant-messenger app for smartphones that claims to "forensically destroy" keys after each message is sent, a practice known as perfect forward secrecy.

Encrypted email is more complicated. Mailvelope, a Chrome and Firefox PGP extension, requires users to manage keys. Without a trusted go-between, however, swapping keys is burdensome. And only a small group of people are willing to forgo the comfort of a Yahoo or Gmail account for crypto-email platforms such as Hushmail and StartMail. It can also be dangerous for one company to handle both messages and crypto keys inside a closed system. Lavabit, a secure email service also used by Snowden, shut down rather than comply with a government demand to turn over a master key that would have exposed emails on its server.

For all these reasons, nobody has nailed email encryption. Ackerly thought he could. He had products for companies in mind, but the broader goal—privacy for anyone with an in-box—was equally important to him and his squad of intelligence-community veterans. They set up shop in a house in Arlington, Va., where pizza boxes, Red Bull cans, and an occasional dead mouse piled up as they reverse-engineered Gmail, Yahoo (YHOO), Outlook, and Mac Mail to create a TDF plug-in. The technology had to be easy to use. A mouse click, no more.

By the spring of 2013 the plug-in was almost ready. Emails were encrypted with perfect forward secrecy, and messages could be set to expire after a period of time or revoked. The sender could control where they were forwarded. Best of all, the plug-in didn't require

anyone to change email providers or open multiple accounts. Recipients of the emails could read an encrypted message without needing to download the plug-in.

The team raised $4 million in angel funding, recruited high-profile advisers like Tim Edgar, who served under Barack Obama as the first director of privacy and civil liberties for the White House national security staff, and moved to nicer digs near Dupont Circle. Ackerly purchased a doormat for the office that said COME BACK WITH A WARRANT.

He didn't mind the intelligence community doing its job. His gripe was with dragnet surveillance. He wanted search warrants to be individualized. In his own case, there was little Ackerly and Virtru could turn over. Since the TDF runs on top of existing email providers, Virtru's servers never see emails, and email providers never see Virtru's AES 256-bit encryption keys. (Several experts confirmed Ackerly's security architecture.) It was end-to-end encryption made easy.

"It's going to make bulk collection programs impossible to conduct," says Edgar, who is now a visiting fellow at Brown and focuses on cyberconflict, privacy, and Internet freedom. "Email is still hugely important to society and business and individuals, but it has resisted all sorts of efforts to make it more secure. What Will Ackerly is trying to do is make it extremely easy for an ordinary user to send an encrypted email and also be able to manage that email. If he's successful and his technology is adopted in a widespread way, it really will revolutionize privacy and security for a huge swath of Internet communication."

Virtru, says an ex–White House privacy czar, will make bulk email snooping "impossible."

Ackerly decided to give away Virtru's basic product for free in the hopes of convincing people to act on their self-described desire for privacy. Users, however, would need to have a pint of trust. The only way to make encryption easy for everyone was for Virtru to act as

an intermediary for keys. For that reason, transparency was paramount. The TDF is open source. Outside cryptologists can vet it and make it stronger. Ackerly hired iSEC, a security firm, to essentially try to hack the plug-in. He also had his friend Weston Hopkins, who'd been on a winning team at DEF CON, the world's premier hacker competition, hammer on the code. "It's good," Hopkins told me.

Then the Snowden leaks happened, and millions of citizens became alarmed at the vast reach of the NSA. They could see now what Ackerly had seen. Still, he hated watching the agency's lifeblood splashed across the media. He felt Snowden could have prompted the same conversation by releasing only a few documents: "He did an incredible amount of damage," Ackerly says. "He gave up so many sources and methods—a blueprint for the adversary." And what would people make of Virtru's NSA pedigree?

Many things changed after Snowden. Companies whose reputations had been criticized for cooperating with the NSA made privacy a priority. Apple decided to encrypt its new iPhone. Yahoo and Microsoft (MSFT) vowed to secure messages. Google made a similar pledge and started work on its own cryptographic extension for the Chrome browser.

None of this pleased the government, which wanted backdoors added to new encryption to help investigations. Cryptologists loathe the idea. Punching holes in security only creates openings for bad actors, in their view. And tech companies fear their products will never be trusted overseas if they provide entry points for American cyberspies. The debate has been playing out in Congress, while in court the NSA battles lawsuits over its bulk-collection programs.

When Virtru launched in beta in January 2014, awareness about privacy was higher than ever, as was the demand for solutions. Ackerly had no trouble attracting clients. Law firms quickly signed up. So did a range of foreign organizations, including an Australian roofing company, a French semiconductor firm, and an Irish political party looking to secure campaign emails. Virtru integrates neatly with Google Apps for Work, which many small

businesses use. For them, encrypted email has often been too costly. Virtru charges $4 per user per month for the professional version of its service, which allows for more control over emails than the free plug-in.

Some experts at firms such as PwC (PWC) and Gartner (IT) have lately been advocating a "data-centric" approach to cybersecurity. As one PwC presentation noted, "Organizations have historically focused on protecting the perimeter to prevent intrusion." If hackers penetrate that perimeter, they can make off with a trove of unencrypted data. By contrast, data-centric security means hackers have to pry open separate encryption for each piece of data. That makes the approach better suited to what PwC called the "model of open collaboration and trust" that is crucial to business and other endeavors. "It's making the data more usable, more accessible, more user friendly," says Jonathan Katz, the director of the Maryland Cybersecurity Center and professor of computer science at the University of Maryland.

The medical community, including New York's Mount Sinai Hospital, has flocked to Virtru, which lets doctors comply with HIPAA and email patients without annoying third-party portals. It also addresses a bigger problem in the health care industry, which is littered with antiquated systems that can't communicate with one another. Patient data comes from many sources and needs to be portable. Because the TDF wraps attachments as well as emails, medical records can be easily exchanged.

The government of Maryland has signed up for the service, along with the Federal Communications Commission. So has one of America's most prestigious newspapers, which is unwilling to go on the record. The publication wants a way to secure sensitive reportage in the cloud. Capital One (COF) and HBO (TWX) are testing Virtru. The latter wants to use it so that its employees and contractors can collaborate across different platforms and safely share not only emails and documents but also video, audio, and images. "We like the integration of multiple platforms on mobile devices and on different

operating systems," says Stephen Fridakis, a vice president of information technology services at HBO. "When you encrypt something, you can say, 'I don't want this forwarded.' We love the fact that it can be revoked. The solution is really portable and not confined to any organization. I can send you an email on your device without you having to think about your public key and my key and doing all these things that are very cumbersome."

And then there is Google. Initially Ackerly was concerned the search giant might not appreciate that Virtru had hacked Gmail. On the contrary, Google executives were impressed. They told Ackerly they'd never seen anyone integrate with Gmail as he had. (Google declines to comment on specific conversations but did not dispute this characterization.) Google has since turned to Virtru as an encryption partner in a booming new market: storing evidence video from body cameras worn by police officers. Google offers cheap space on the cloud, while Virtru keeps the video safe and reduces liability. Some Google salespeople are recommending Virtru as an encryption solution to their Google Apps for Work customers. As of August more than 2,000 companies using those apps were securing emails with Virtru. Another 1,000 not using the apps also use Virtru.

The company declines to disclose its revenues, but each user of its "pro" product brings in $48 a year; the average company using Google Apps has about 100 employees. The technology should be easily scalable: Virtru stores only encryption keys (at low cost), which keeps overhead minimal. The company says it has 90% gross margins. "All we really pay for is managing the keys," says John Ackerly.

It is John, Will's 41-year-old brother, who is Virtru's CEO, the one focused on running the business. His role frees Will to devote himself to technology—and to periodic flights of fancy. The partnership seems to work, though John, a Rhodes Scholar, Harvard Business School grad, and former private equity executive, can find his patience tested by his brother's ways.

In May, for example, Will disappeared for 72 hours and missed an important sales meeting. John's repeated calls went straight to voicemail. Eventually John discovered that his brother had been holed up in his apartment, a few blocks away from Virtru's offices. John marched over to chew him out, but before he could start, Will—bleary and disheveled after multiple all-nighters—said, "Let me show you something." He spun his laptop around and explained that he had figured out a way to make encrypted emails searchable, something that previously wasn't possible on widely used consumer platforms such as Gmail.

"Let me show you something," Ackerly said. He'd found a way to search encrypted emails.

Right before launch, Virtru commissioned a Harris poll of more than 2,000 Americans. Nearly half felt restricted in what they could say over email because it might be read by someone other than the intended recipient. But few have taken even the first step to protect themselves.

"Never has this been more timely," says Nuala O'Connor, the president of the Center for Democracy and Technology, which describes itself as a "champion of global online civil liberties." Says O'Connor: "We've got to make the user interfaces manageable for the ordinary citizen. That's the tipping point. The guys at Virtru are trying to solve for that."

O'Connor thinks online behavior will change when simple tools like the TDF are widely enough in use. Ackerly hopes that's true. Meanwhile the Virtru team continues to add features and polish the product, including prompts to encrypt when a credit card number or other sensitive data is detected.

In August a different sort of overture landed in Ackerly's in-box. He suspected it might happen one day. The message was from a federal intelligence and security agency. It wasn't

a warrant, and the feds weren't asking for an encryption key. They weren't even connecting to chide Ackerly for rolling out strong encryption to the world. No, the government had a different agenda: It finally wanted to use his TDF.

Luke O'Brien is the senior correspondent at POLITICO Magazine and a former senior writer at Deadspin. He has also written for Fast Company, Details, Slate, Rolling Stone, GQ, and ESPN.

To see the full list of the Fortune 40 Under 40, visit fortune.com/40-under-40.

A version of this article appears in the October 1, 2015 issue of Fortune magazine with the headline "The anti-hacker."