THE NEW YORKER

A CYBERSECURITY FIRM'S SHARP RISE AND STUNNING COLLAPSE

Tiversa dominated an emerging online market—before it was accused of fraud, extortion, and manipulating the federal government.

By Raffi Khatchadourian October 28, 2019

0:00 / 1:36:46

Audio: Listen to this article.

I. THE FOOTBALL

Before Robert Boback got into the field of cybersecurity, he was a practicing chiropractor in the town of Sewickley, Pennsylvania, twelve miles northwest of Pittsburgh. He was also selling used cars on eBay and flipping houses purchased at police auctions. The decision to branch out into computers came in 2003, after he watched a "60 Minutes" report by Lesley Stahl about pirated movies. For years, while digital piracy was devastating the music industry, Hollywood had largely been spared; limitations on bandwidth curtailed the online trade in movies. But this was changing, Stahl noted: "The people running America's movie studios know that if they don't do something, fast, they could be in the same boat as the record companies."

Boback was thirty-two years old, with a Norman Rockwell haircut and a quick, smooth, entrepreneurial manner. Growing up amid the collapsing steel industry, he had dreamed of making it big, hanging posters of high-priced cars—a Lamborghini, a Porsche—on his bedroom wall and telling himself that they would one day be his. After high school, he trained to be a commercial pilot, imagining a secure, even glamorous, life style—but then the airline industry began laying off pilots, and he switched to chiropractic, inspired by a well-off practitioner his family knew.

Watching "60 Minutes," Boback saw a remarkable new business angle. Here was a multibillion-dollar industry with a near-existential problem and no clear solution. He

did not know it then, but, as he turned the opportunity over in his mind, he was setting in motion a sequence of events that would earn him millions of dollars, friendships with business élites, prime-time media attention, and respect in Congress. It would also place him at the center of one of the strangest stories in the brief history of cybersecurity; he would be mired in lawsuits, countersuits, and counter-countersuits, which would gather into a vortex of litigation so ominous that one friend compared it to the Bermuda Triangle. He would be accused of fraud, of extortion, and of manipulating the federal government into harming companies that did not do business with him. Congress would investigate him. So would the F.B.I.

But as Boback was watching "60 Minutes" all he saw was a horizon of possibility. Stahl pointed out that pirated music and movies were spreading primarily on peer-to-peer networks—an obscure precinct of the Internet that was sometimes called the Deep Web. The networks were made up of hundreds of thousands of decentralized connections, in which one computer was linked to no more than five others, and then through those five computers to many more, expanding exponentially like the branches of a large tree. These connections were invisible to search engines like Google. Even the software that allowed users to browse them had only a limited field of vision—glimpsing just random fragments of the tree at a time. Boback wondered if it was possible to design a system that could scan the whole tree at once, then block people from sharing files on it. Certainly, this capability would be worth a lot.

Boback had no idea how to build such a thing, but he knew someone who might: a patient of his, Sam Hopkins, whose girlfriend had persuaded him to pursue chiropractic treatment after a car crash. Hopkins was in his thirties, too. He was soft-spoken, with a childlike disposition, a wispy physique, and a goatee. He had grown up in inner-city Pittsburgh, in a home where money was scarce. As a boy, he had taught himself how to program on a Commodore 64 that was on display at Sears. Bored with school, he dropped out, and built an Internet-service provider, which was sold to a local telecom company. By the time of his car accident, he was designing high-speed computer networks for Marconi Communications.

When Hopkins came in for treatment, Boback explained his idea, and after some thought Hopkins said that it could be done. At that time, the most popular peer-to-peer software was a free application called LimeWire. When a user searched for a file—

say, an MP3 of "Hey Ya!"—LimeWire sent a query to other users asking for it. If the file turned up, this meant that someone had designated it for sharing. The main peer-to-peer network limited the number of computers a person could search. But Hopkins told Boback that the limitation could be overcome with a system that scattered virtual users, or "nodes," throughout the network—in effect emulating many, many copies of LimeWire running simultaneously. With enough nodes, the whole network could be seen.

That Christmas holiday, Hopkins locked himself in a room to program, and in a couple of weeks built a rough prototype. Even though it could maintain only a small number of nodes, data flowed through it in a torrent. The system could track the search terms that thousands of users were entering—offering unique insight into what was in demand, half clandestinely, on the Deep Web. The terms filled the screen so rapidly that Hopkins had to program a "decelerator" to slow them down. Watching the words race by, the two men began to suspect that they had genuinely struck it big.

By the end of the year, Boback and Hopkins were sitting in the well-appointed offices of a Pittsburgh law firm that specialized in intellectual property. The attorneys were optimistic. Rather than charge billable hours, they offered to work for ten per cent of the proceeds when the system sold. One said that the deal could be worth fifty million dollars. With the firm's help, Boback and Hopkins formed a corporation. Hopkins came up with its name, Tiversa, a portmanteau of "time" and "universe." It was also an anagram of *veritas:* Latin for "truth," but scrambled.

Boback is a storyteller. Words pour out of him in cascades that, depending on the listener, can register as beguiling, slick, questionable, or bullshit. One colleague described him as "very confident, sometimes bordering on cocky." Another told me, "He was a master manipulator. Watching him was like watching van Gogh use oils."

As Boback began marketing his system, he landed a big meeting with lawyers representing the Recording Industry Association of America, but the lawyers said they already had a strategy to combat file sharing: sue the problem into oblivion. Undeterred, he and Hopkins flew to Los Angeles, where they met with Darcy Antonellis, the head of anti-piracy efforts at Warner Bros. The studio was gearing up to release a summer blockbuster, "Troy," an epic in the mold of "Ben Hur," rumored to have cost almost two hundred million dollars. A screener had already leaked, and, during the meeting, Boback strove to convey how much money Warner Bros. was losing: in his hotel room beforehand, Hopkins had added to the software a digital counter that appeared to track downloads of "Troy," tabulating a fifteen-dollar loss with each one. Boback explained that the system, which he was calling Media Spy, could be designed to jam the activity. Antonellis listened patiently, and then said that it seemed too good to be true. She meant it literally. Such an intrusion would require Warner Bros. to block people from

posting files at the point of their computers, which she suspected was legally impossible.

After the meeting, Boback's lawyer mentioned that a partner in his firm knew Orrin Hatch, the chairman of the Senate Judiciary Committee, who had spoken out against pirated music and movies. Perhaps, if Hatch gave his imprimatur to the system, the concern about its legality could be overcome. That May, Boback and Hopkins drove to Washington with another lawyer in the firm, to meet with Hatch in a conference room in the Hart Senate Office Building. They brought a laptop and made their pitch, as Hatch listened with polite interest. While wrapping up, they explained that their system could track not only music and movies (the vast bulk of the content on peer-to-peer networks) but anything else that people were sharing: documents, spreadsheets, PowerPoint decks. Some of those items appeared to have national-security implications, so Hopkins had created a second user interface for the software, called Patriot Spy. Boback shared a few examples of what the system had found, including files belonging to a person in Australia who had jihadi literature and bomb-making manuals.

"Stop what you're doing," Hatch said. He led his guests to his office, seated them in faux-leather chairs, and commanded an assistant, "Get me George Tenet." Within a few minutes, the director of the C.I.A. was on speakerphone, and Hatch was telling him that, if the agency did not have the capability he had just witnessed, then it should. Boback and his colleagues looked at one another in disbelief. By the end of the call, Tenet had invited them to visit the C.I.A.'s headquarters, in Langley, Virginia, first thing the next morning.

Unprepared to spend the night, Boback and the others bought clean underwear and toothbrushes, then tried to find a hotel in D.C. They were laughed out of a downtown Marriott, and eventually landed in a tumbledown joint on the city's outskirts. Still, they were giddy. If the C.I.A. wanted to buy their system, then Hollywood could wait.

In the morning, they pulled up at the front gate of Langley and explained that they had an appointment with the head of the Directorate of Science and Technology. They were sent to the Original Headquarters Building, but Boback made a wrong turn and the car was soon surrounded by security personnel, their weapons drawn. A guard

warned them to leave immediately. "Do you understand?" he screamed. Boback, unsure whether the guard meant the road they were on or the entire property, rolled down the window. "No," he said. "Can you explain it to us?" The other passengers were terrified, but Boback was unfazed. As he turned the car around, he said, "We got to get in here. It's the meeting of a *lifetime!* "

Inside, the head of the Directorate of Science and Technology was joined by an official representing In-Q-Tel, a corporation that the C.I.A. had set up to fund new technologies. (The "Q" refers to the technician in James Bond films.) A follow-up call from one of the participants led to more trips to D.C., and suddenly Boback and Hopkins were journeying through the shadow world of the post-9/11 national-security establishment.

There were visits with the F.B.I. and the military. They returned to Langley, to meet with another enthusiastic official, who introduced himself only as Bad Bob. The agency also instructed them to go to a Starbucks in Reston, Virginia, from which a C.I.A. officer would convey them to a secret facility. The officer drove them for several minutes before arriving at a large building, where they gave a presentation in a packed room. One audience member asked if they were prepared to sell, and, as they headed back to the car, the officer pressed them to name a price. Hopkins said, "I'm thinking two billion dollars," which prompted laughter, and some advice: sell your technology to a large contractor, like Raytheon; don't deal with the government yourself.

On the drive back to the Starbucks, Boback asked what prevented the C.I.A. from simply stealing their technology. The officer told them, "If you weren't an American citizen, I would have already stolen it—and, oh, you have a connection to Senator Hatch." The offhand comment sent a jolt of paranoia through Boback and Hopkins, who began to refer to their laptop as "the football"—the White House term for the briefcase that allows the President to access the nuclear codes. They decided to secure the software. At the time, Hopkins lived on thirty-eight acres that he had converted into a makeshift wildlife sanctuary. He burned the code to a DVD, and then walked out and buried it.

The more that intelligence operatives expressed an interest in the technology, the more Boback sought to prove its value. He and Hopkins renamed the system EagleVision X1—a reference to the "X1" markings on some classified files. When

Boback saw an apparent spike in searches containing "Chechnya" and "jihad," he let Bad Bob know. When he saw a file suggesting that an attack might be imminent in Egypt, he told a congressman.

EagleVision X1 had been designed to comb the peer-to-peer networks using search terms that Hopkins set for it. But, as Boback tried to market the software, Hopkins worked to improve the system, so that if it had a hit on a search term then it would automatically pull down everything else that was being shared on that computer. New material flooded in. EagleVision X1 found a document in China belonging to the F-35 Joint Strike Fighter program. It also pinpointed a man, about an hour from President George W. Bush's Texas ranch, who was sharing files about sniper rifles and photos of the President's daughter. Boback notified the Secret Service, and early the next morning agents turned up at Boback's home.

At first, Boback assumed that anyone who willingly shared this kind of information must be engaged in some kind of illicit trade. But, as Tiversa's system vacuumed up more examples, he learned that there was a surprisingly benign reason. LimeWire and its competitors were confusingly designed, causing people hunting for music to open up their hard drives—inadvertently designating sensitive files for sharing on peer-to-peer. In pursuit of a free MP3, jihadis and federal contractors, soldiers and diplomats, executives and celebrities were doxxing themselves. Because the people who used LimeWire were looking almost exclusively for music, this mass exposure had gone largely unnoticed.

Despite Boback's hustle—or perhaps because of it—he struggled to sell EagleVision X1 to the C.I.A. With the chance of a big payout receding, Boback thought that perhaps the technology would be easier to sell if he built a business around it. So, in 2005, he met with a Pittsburgh financier, who agreed to invest seed money to elevate Tiversa from some lines of code into a startup. The investor recommended that Tiversa focus on corporate clients; they could bring in agencies like the C.I.A. later.

Boback rented office space in a Pittsburgh suburb, and took on his first full-time employee, a Wharton graduate, who started trying to bring order to his vision. The two clashed. In 2005, no one at Tiversa was taking a salary, and, to stay afloat, Boback spent much of his time at his chiropractic practice. (In addition to seeing patients, he had to fight to keep his license: the Pennsylvania Board of Chiropractic briefly suspended it,

because he was unable to prove that he had completed an education requirement.) When Boback was in the office, his freewheeling style was often at odds with normal business practice. He admitted to me that, early on, Tiversa installed phony computer towers—plastic shells with blue lights "that literally did nothing"—to give visitors the impression that his software required more powerful hardware than it did. Sometimes he inflated the number of his employees, by having friends occupy desks in the office. Tiversa's early literature referred to its Pennsylvania office as its "World Headquarters." (The company had no other facilities.) "We had no credibility in the space," Boback told me. "We wanted to make it look as good as we could."

In 2006, a more significant investor signed on: Adams Capital Management, named for its founder Joel Adams, a Pittsburgh venture capitalist. Several years earlier, Adams had put his money into a scrappy startup that marketed laser technology, and later it sold for more than a billion dollars—a "unicorn," in investor parlance.

Adams Capital invested more than four million in Tiversa, and helped secure an all-star board of advisers. Maynard Webb, the former eBay executive and chairman of Yahoo!, joined, and he brought on other executives from Silicon Valley. Howard Schmidt became an adviser, and soon afterward was appointed the cybersecurity czar for the Obama Administration. General Wesley Clark, the former Supreme Allied Commander of NATO, came on, and developed a good rapport with Boback, who sold his practice to devote himself to Tiversa full time.

Tiversa's prominent supporters quickly helped Boback assemble an impressive client list: Capital One, Lehman Brothers, Goldman Sachs, American Express. The companies were paying for a monthly monitoring service, in which Tiversa scanned for breached corporate information, or the personal data of top executives. By this time, EagleVision X1 could access more than a million users, and its capabilities were expanding. Because peer-to-peer networks were constantly in flux, as people turned their computers on and off, Hopkins had designed a stable repository for the system, which became known as the Data Store. EagleVision X1, programmed with search terms that were set for clients (for instance, "Lloyd Blankfein," for Goldman Sachs), would scour the networks, then deposit what it found in the Data Store. Each file was labelled to indicate when it was downloaded and what I.P. address it came

from, so that its behavior could be tracked—if it remained in the same location, or if it was being shared, or if it suddenly vanished.

As the company matured, Boback created an "ops room," where Tiversa analysts probed the Data Store for files related to clients. Over time, the room evolved to resemble a set from "The Bourne Identity"—a darkened space with electric-blue lighting, a window that could be triggered to go opaque, and a retinal scanner at the entrance. Tiversa's analysts took special care to see if any files appeared to be "spreading"—passing from user to user, out of the company's control.

American Express had the largest contract, paying a monthly fee of about seventy-five thousand dollars. Once the money began to flow, Adams Capital valued Tiversa at seventy million dollars. Along with the revenue, the company began to gain attention. In 2007, the House Committee on Oversight and Government Reform scheduled a hearing on inadvertent file sharing; it invited Boback to testify, and he asked Wesley Clark to join him.

To prepare, Clark asked if there were classified documents on the Deep Web. Boback pulled up two hundred marked "SECRET," including information about lifesaving technology to neutralize radio-controlled bombs. Clark notified an intelligence official in the White House, who noted, with alarm, "They're in full color!" A week before the hearing, Boback contacted Clark to report that Tiversa had located records pertaining to the Defense Department's network for handling classified material. They were on the home computer of a contractor who was using LimeWire.

At the congressional hearing, Clark brought up the tranche of records, calling it "sort of a hacker's dream," though no one, of course, had hacked them; they were just sitting there in public view. He also emphasized that potential victims often had trouble understanding the issue. EagleVision X1 had found a contractor's threat assessment of American cities—a catalogue of weak points that an enemy might attack. "We immediately contacted the contractor, and the city," he said. "They denied the problem. They don't understand what has been leaked."

Seated beside Clark, Boback gave an expansive list of what a motivated searcher might find: "Federal and state identification, including passports, driver's licenses, Social Security cards, dispute letters with banks, credit-card companies, insurance companies,

copies of credit reports." The documents, he alleged, had been harvested in Pakistan, Africa, and Eastern Europe, from foreigners who were "grabbing this information." Only a few years earlier, he was fixing lumbar problems and selling cars on eBay. Now he was explaining to the country's top lawmakers, "This is the new threat to information security."

II. WALDO

At about the time that Boback and Hopkins realized that governments and businesses were hemorrhaging information on the Deep Web, so had another man, living thousands of miles away. Richard Wallace grew up in rural Idaho, among family members who struggled with addiction. His mother's life was consumed by pills, and two siblings would eventually die from overdoses. In a chaotic home, he developed the habit of helping people around him. After high school, he moved to Spokane, to train as a firefighter. There, he met Amy Speelmon, an R.O.T.C. student at Gonzaga University, and they were soon married. After 9/11, Amy deployed to a garrison in Germany. Wallace put firefighting on hold and joined her.

In Germany, Wallace strove to find his place. He was too independent-minded, too odd, to thrive as a military employee. But he was inclined to serve, and when his skills were acknowledged—particularly by people with authority—he was eager to please. Wallace volunteered to oversee the personal effects of soldiers killed in Iraq and Afghanistan. It was grim work that no one else was enthusiastic about doing, and he was commended for it.

To relax, Wallace often turned to his computer. Before moving, he and Amy had been watching "The Sopranos," and at the garrison he began to hunt for pirated episodes. Exploring the Deep Web, he found that many members of the armed forces had downloaded peer-to-peer file-sharing programs, and were inadvertently exposing files: records of troop movements, accounts of I.E.D. attacks, and intelligence summaries. He helped the military identify which computers were leaking.

In 2004, the Wallaces relocated to western Illinois, where Amy worked as an R.O.T.C. instructor. Rick stayed home with their children (they eventually had five), and farmed, a little. He also kept his head in his computer. He had exploited a loophole in LimeWire that allowed him to crawl across the network, a solitary digital explorer. He

sent the military more tips, and began to warn civilians about breached files, too. A neighbor suggested that he channel his expertise into a business, but entrepreneurship wasn't in his nature; he was a volunteer. When Hurricane Katrina hit Louisiana, he drove down to assist FEMA and spent weeks helping to sort out the wreckage.

Wallace never asked for payment from the people he warned, and, perhaps as a result, they were often suspicious of his motives. To give his efforts legitimacy, he created a Web site, seewhatyoushare.com, where he blogged about his work. He sent some items to Matt Drudge and Michelle Malkin, conservative pundits he admired, and he says that they responded gratefully. Eventually, he caught the attention of Thomas Sydnor II, a former Senate staffer who had sat in on Boback's meeting with Hatch. Sydnor had gone on to work at the Patent and Trademark Office, but he remained interested in inadvertent file sharing, and began checking in with Wallace, whom he considered one of the few people who understood the dangers.

Peer-to-peer networks were awash in child pornography, and Wallace had been issuing warnings on his Web site. Sydnor told him to stop trying to track such images, because possessing them is a crime, no matter what the reason. Sensing that Wallace could use a more structured outlet for his work, he mentioned him to Boback. Annoyed, Boback told Hopkins, "He is ruining our credibility by just being out there winging it with these calls." The two men considered hiring Wallace, merely to eliminate competition, but on reflection wondered whether he might also have something productive to add. Tiversa had only one full-time analyst, and though he had conventional skills—he had worked at Microsoft—he lacked deep experience with peer-to-peer networks. Boback flew Wallace in for an interview, and was struck by his offbeat manner, but he reasoned that this was common in cybersecurity. Two weeks before the congressional hearing, Wallace moved his family to Pennsylvania and started work, racing to dig up material that Boback could use in his testimony.

Tiversa's office culture, Wallace quickly discovered, was anything but formal. Early on, Boback had instituted a rule: new hires were bestowed a sword representing their character. Tiversa's chief technology officer was given a samurai's *katana*. Another employee got Gandalf's sword, from "The Lord of the Rings." Boback planned outings to a shooting range and sometimes came in with a pistol. Once, he displayed his gun to an executive who had challenged him. As the executive later recalled, Boback "sat at a

desk in front of me and reached into his sock holster and pulled out a revolver and showed me its features."

Wallace quickly adapted to the unconstrained atmosphere. Hired as an analyst, he helped comb the Data Store for client information, but he also commandeered an independent DSL line to run manual searches in his old way. He was often able to find files that EagleVision X1 could not, and the company's software developers began studying his methods to improve the system's code.

Soon after the congressional hearing, Wallace made a discovery that captivated Boback's imagination: someone was sharing suspicious financial documents, along with images of gold bars and passports. The I.P. address belonged to a lawyer in California, who was touting investments that could return forty per cent a week. Boback, who suspected that the investments were a fraud, had the files printed; then he and Wallace, like detectives, spread the pages out on a table to study them. They spent weeks on the project, hoping to somehow earn money from the discovery.

Ultimately, there was no way to gain from it, but for Wallace the episode demonstrated the value of his idiosyncratic skills. For Boback, the puzzle was thrilling. He was an avid gambler. Often, he would stride past Wallace's desk and summon him to leave, saying, "Waldo, you're with me." Wallace typically didn't know where they were headed, but often the destination involved bets. An employee who worked closely with Boback later told the F.B.I. that she thought he was a gambling addict. (Boback denies this.)

A strange intimacy grew between the two men. There were flurries of texts at all hours, games of Halo past midnight. To others, they seemed to inhabit an atmosphere of semi-continuous scheming. The office had a window overlooking a parking lot near a Red Roof Inn. Wallace noticed a woman who often turned up to wait for a man—another puzzle that became the topic of speculation, jokes, even a mock stakeout.

At times, Boback had conflicts with peers. As a former Tiversa employee told me, "The Bob that he presents to people he just meets—that Bob is very charming, very likable, very engaging. Then, there is the person behind the mask, who is a little bit paranoid, angry, untrustworthy, greedy, generally not a nice person. If you got on his bad side, you stayed on his bad side." Wallace began supporting Boback in conflicts. After an employee argued with him, colleagues say, Wallace designed a simulated F.B.I. arrest

report, indicating that he had groped someone on a flight, and circulated it within the company. (Wallace denies this.) "Rick became Bob's puppet," another former employee told me. "Bob completely controlled him."

Boback also clashed with Hopkins's wife; she had helped start the company, but then became openly distrustful of Boback. Wallace found a clip of a porn actress who resembled her and joked with Boback about adding her name and phone number and sharing it on peer-to-peer.

Wallace says that he and Boback also purchased a G.P.S. tracker to surveil her. "We snuck over to her car, stuck it on, and watched her go to a place in Indiana," he recalls. "She had a boyfriend there. So then Bob pulled Sam into the office, and goes, 'Well, I hired this private investigator to see what's going on. I just wanted to let you know.' Of course, Sam reacts terribly, goes home, has a big fight. Sure enough, they get a divorce. Bob takes credit for it."

Boback now tends to claim that any bad behavior at Tiversa was caused by Wallace going rogue. He told me that he ordered the G.P.S. device because he suspected that members of his sales team were defrauding Tiversa. "They were charging mileage on *everything*, and I was, like, *come on*, you're getting paid a commission!" he said. "So I was, like, I'm going to get a G.P.S. I want to see how far these people are driving. I ordered it, got it. Wallace saw the G.P.S. sitting there, and then, without any knowledge of mine, when Sam was going through his divorce, Wallace put it on her vehicle. Now, I did know that he put it on that vehicle—*after*—because he had told me, and I was, like, 'You shouldn't be doing this, get it off.' Which he did."

Within a year at Tiversa, Wallace had taken on a new title, director of special operations. He continued to work as an analyst, but also spent hours on the DSL line searching for government files, or for documents with criminal implications. This work had no immediate business value, but Boback hoped that it could serve as a proof of concept, to help secure a federal contract.

Most people in the office knew little about how Wallace spent his time, but he was quietly achieving something remarkable. He passed on tips to the C.I.A., the Secret Service, the Treasury Department, the military, and the F.B.I.'s Pittsburgh field office, which began sending a special agent to Tiversa almost weekly to coördinate with him

on child-pornography research. Wallace also sent the Bureau evidence of online identity theft: I.P. addresses that seemed to be harvesting Social Security numbers or credit-card information.

Sometimes, frustrated by the slow pace of federal law enforcement, Wallace fed his tips directly to police departments. In 2013, the Law Enforcement Executive Development Association, a national training organization, presented him with an award for assisting in hundreds of cases. (The F.B.I. recognized his efforts, too, in a ceremony conducted by Robert Mueller, near the end of his term as director.) Steven Pickett, who worked a dozen cases with Wallace as a deputy sheriff in Mississippi, told me, "He is a real unsung hero from another world."

Wallace's research opened doors into law enforcement for Boback, but it became clear that the men had different ideas about it. Once, Wallace discovered child pornography on a computer at a Catholic seminary, and told the F.B.I. Boback, he says, saw a business opportunity, and called the seminary's director to pitch Tiversa. (Boback disputed this, saying, "I reached out and told him the problem, and he immediately said, 'Oh, my gosh, we are going to address it immediately.' There was never a 'Here's how much it's going to cost.' No contract discussed!") The director notified the F.B.I., too, and Wallace soon got a call from the special agent he worked with in Pittsburgh, angrily warning him that Tiversa should never pull a stunt like that again.

III. FUD

For most of us, computers are effectively magic. When they work, we don't know how. When they break, we don't know why. For all but the most rarefied experts, sitting at a keyboard is an act of trust.

A human-to-machine relationship defined by estrangement offers a unique sales opportunity: fomenting anxiety turns out to be an excellent way to draw in clients. One of the first people to identify the tactic was the director of I.B.M.'s Advanced Computing Systems Laboratory, Gene Amdahl, who left his job in 1970 to build machines that could run I.B.M. software more cheaply. As Amdahl went to market, he learned that his former employer was warning potential customers that any hardware not made by I.B.M. was fraught with risk. The feeling that I.B.M. was hoping to inspire, Amdahl noted wryly, was "FUD"—fear, uncertainty, and doubt. The name stuck.

In the nineties, Microsoft pursued a canonical FUD strategy, creating phony error messages to make consumers wary of using Windows on a competitor's operating system—a tactic that resulted in a legal settlement exceeding two hundred million dollars.

In cybersecurity, where ordinary digital anxiety is compounded by esoteric threats, the use of FUD to generate business is especially notable. Misleading tactics—dubious assessments and glossy graphics supported by underwhelming data—have become so common that one researcher recently went online to chide colleagues to "cut the FUD." The practice thrives because a small system failure can carry tremendous financial risk, and the immediate customers of cybersecurity services are often corporate executives, not technical experts. Given that a publicized breach can damage both a corporate brand and a career, it is safer to pay a security firm and tell no one outside the company.

"If you're told that cyber security attacks are purported by winged ninja cyber monkeys who sit in a foreign country who can compromise your machine just by thinking about it you're going to have a fear response," the technical director of the British National Cyber Security Center recently noted. "The security companies are incentivized to make it sound as scary as possible because they want you to buy their magic amulets." Among firms that occupy the gray zone between outright hacking and responsible behavior, FUD can drift into criminality: threats by innuendo, extortion.

Boback quickly intuited the possibilities that FUD could offer a skilled sales force. He pushed his staff to emphasize to potential clients that their businesses were inextricably linked to venders and customers, which meant there was no way they could close all their points of exposure. He encouraged dire warnings of "file spread," even though it was rare for users to pass around anything but music. At Tiversa, file spread was sometimes called "digital wind," as if it were a natural phenomenon that could not be controlled. Key to Boback's pitch was that Tiversa had a singular ability to track the wind across millions of computers. That was true—but this unique capability meant that almost no one outside his company could verify his claims.

In early 2008, Boback called Wallace into his office, shut the door, and told him that the American Express account was in jeopardy. With Tiversa's help, Amex had eliminated the significant data breaches on its network, and now it wanted to drastically reduce its fee. If this happened, Boback might not be able to make payroll.

Wallace later told the F.B.I. that the two men devised a strategy to convince Amex that the threat remained urgent: they would make it seem as though Tiversa had detected Amex files involving hundreds of invitation-only credit cards being shared overseas and among suspected criminals. To make this believable, Wallace secretly altered the Data Store, to give the appearance that the files had spread. In some cases, he used "burnt" I.P. addresses, from computers shut down by law enforcement because they had been involved in scams or in child pornography. Once they were taken offline, there was no way to confirm what was attributed to them. Amex ended up replacing the cards, at the cost of a million dollars, but it did not renew its contract.

Boback denies conspiring with Wallace, and claims that there was never any fraud at Tiversa. But Wallace says that in 2008 he began to systematically plant false spread in the Data Store to inspire FUD among prospective clients and to promote Tiversa's technology. That summer, Wallace was given a performance review, praising his work: "Rick always seems to be able to find a hard hitting file or P2P situation to accelerate our client acquisition."

Around that time, Wallace stumbled on an I.P. address in Virginia that was sharing a file with hundreds of Social Security numbers belonging to prominent people around Washington, D.C., including Stephen Breyer, the Supreme Court Justice. Immediately, Wallace pulled down everything that the address was sharing. The tranche included documents on letterhead from the Wagner Resource Group, an investment firm in McLean—clearly the source of the breach. "Bob was standing right behind me," he recalled. "He said, 'Don't tell anyone.' " Boback's plan, Wallace told the F.B.I., was to call the Wagner clients whose information had leaked, pretending to be investigating the breach. After angry clients began putting pressure on the firm, Tiversa could make a sales pitch.

Midway through the effort, the company's founder, Phylyp Wagner, phoned the Tiversa offices, eager to talk, but Boback refused to take his call until more of his clients were reached. (Boback told me that he was earnestly trying to locate the source of the leaked files.) When the two men eventually spoke, Wagner later recalled, Boback told him that his files had spread to Asia, suggesting that criminals there were using them to manufacture credit cards. After the call, Wallace manipulated the Data Store to support the story, and the fraudulent data were written up in a report. The following day,

Wagner, desperate to protect his clients, agreed to engage Tiversa. "These are people I've known for years," he told me. "So exchanging money for their well-being—I'm willing to do that."

For Tiversa, this was an extraordinary promotional opportunity: a Supreme Court Justice had just had his Social Security number exposed by the very problem that Boback's business was set up to fight. But Tiversa had signed confidentiality agreements with Wagner, and so there was little it could reveal openly. Wallace says that he and Boback concocted a new plan, to use a false persona to tip off the press. Wallace had just the thing: an alias, Glen Breakwater, that he had briefly used on his old Web site. (Later, he created a Facebook profile for Breakwater, casting him as an African-American fan of Michael Jackson and Tyler Perry. The profile was a barely coherent pastiche of stereotypes, but it attracted friends, some of whom still send birthday greetings.)

Wallace, using a burner phone and masquerading as Breakwater, called the Washington *Post* to leak the story. The resulting article, which ran under the headline "JUSTICE BREYER IS AMONG VICTIMS IN DATA BREACH CAUSED BY FILE SHARING," noted that the files were downloaded as far away as Colombia and Sri Lanka. Wagner told the *Post* that this news was "devastating." The story pointed out that Tiversa had been brought in to remediate, and quoted Boback, saying that Wagner's clients had been "at a very high risk, almost imminent, of identity theft."

Wagner's files were like a briefcase forgotten on a train but recovered moments later. The company had failed to secure its clients' data, but there was no apparent harm: no one outside of Tiversa seemed to have noticed the slip. Later, a Tiversa employee on the Wagner account conceded, "I don't think we ever saw the files reappear" on the Deep Web. But, by signalling that the files had spread, Boback had concocted a potent marketing parable: inadvertent file sharing could have dire consequences.

After the *Post* story ran, Boback and Wallace drove to Fairfax, Virginia, to meet Wagner at a bar. Wallace later recalled that he was so preoccupied by the lie he had helped engineer that, as he crossed the street from their parking spot, "I damn near got hit by a bus." While the men talked at the bar, he said, he fantasized about what might happen if Boback were called away for a moment: "I would have slid right over to Phylyp, and said, 'This is the biggest sham ever.' But I never got the opportunity. Then

I thought that I was glad I didn't do that. I would have been fired on the spot." Boback denies any wrongdoing concerning the account. Wallace told the F.B.I. that, on the drive back to Pittsburgh, Boback joked about how Wagner had been "fucked."

With Amex withdrawing, Tiversa scrambled to sign up new customers. But, Boback told me, "we were exhausting the contacts who were helping us get to clients, the economy was starting to get a little dicey, and budgets were tightening up." He was convinced that the problem was communication. Boback's sales technique often involved hinting at an ominous data breach, then withholding details until potential clients paid, and on a number of occasions the approach had backfired. G.E.'s information-security team felt it was being extorted. PNC Bank contacted the authorities. Boback believed that these reactions were misdirected animus: companies were blaming Tiversa for their own security failings. He began to wonder, "How do you deliver a message without having a shoot-the-messenger-type response?" That February, a Tiversa analyst unwittingly provided an answer—a clandestine way to publicize data breaches. In an e-mail, he told Boback about a Web site called WikiLeaks, which had launched two years earlier and was attracting attention. "It claims that postings are untraceable," the analyst explained.

Several weeks later, Wallace says, Boback told him on short notice to prepare for an overnight trip: they would fly to Atlanta and pick up a Mercedes. He added, incongruously, that Wallace should make sure to bring his computer. They retrieved the car, and on the drive back to Pennsylvania Boback asked if it was possible to use a Wi-Fi router that someone had left unprotected to submit files culled from peer-to-peer to WikiLeaks; if it was, then Tiversa could use the uploads to illustrate the need for its protection.

In Charleston, Wallace later told federal investigators, Boback pulled off the highway to look for an open router, and found one near a suburban development that was under construction. Both men were spooked and exhilarated. Boback told Wallace that he needed to use a nearby Port-a-Potty, while Wallace started his laptop and began the transfer. When a police car drove by, Wallace threw a blanket over the laptop and continued working beneath it.

Wallace uploaded to WikiLeaks an Airbus business agreement; a spreadsheet of Chevron's assets in Canada; Dyncorp schematics for a military camp in Afghanistan; a

Defense Department manual on data protection; and other documents from a folder he had named "Files for the bus"—indicating that any company with records inside could get thrown under one. On a later trip, Wallace uploaded more files to WikiLeaks, from a Starbucks in Indianapolis.

Among the most sensitive files that Wallace says he submitted were two classified technical studies of a jammer that the Army had used in Iraq to disrupt radio-controlled bombs—evidently drawn from the same tranche of documents that had alarmed Wesley Clark. Their publication triggered some of the first real criticism of WikiLeaks. Even though the jammers had largely been replaced by a newer model, there was no obvious point to revealing the way they worked, no wrongdoing exposed. As the Washington editor for *Ars Technica* wrote, "The decision to run with this one is just utterly baffling."

Wallace later said that submitting documents to WikiLeaks was a low point in his life. Boback spoke about the uploads in the same gleeful way that he had spoken about other escapades. "I remember him talking about how they were going to be rich after all this broke," one person recalled. As WikiLeaks began publishing the documents, Boback sent an e-mail to Tiversa executives, urging them to pitch the affected companies, "before some IT goon in the organization tries to convince them that they have it covered."

Boback disputes just about everything in Wallace's account of the trip. The first time that I discussed WikiLeaks with him, he told me, "We had no interaction with them." Then he paused, and added, "Directly." After another pause, he said, "That we know of." Later, when I pressed him about the uploads, he offered a confused set of denials, saying flatly that they did not happen, but also that Wallace may have performed them without his knowledge. I told him that I intended to gather more information, and his voice sharpened. "Check it!" he demanded. "You will see it was not from a Tiversa I.P. address."

IV. MARINE ONE

In the summer of 2008, Boback got an unexpected break, when an intermediary connected Tiversa with LifeLock, the identity-theft-protection service. The match

was logical. Tiversa had patented technology but limited sales. LifeLock was adept at marketing but had no intellectual property.

MORE FROM THIS ISSUE

NOVEMBER 4, 2019

A CRITIC AT LARGE

Why We Can't Tell the Truth About Aging

By Arthur Krystal

OLD WEST DEPT.

Waiting for Kanye in Wyoming

By Corey Morris

SHOUTS & MURMURS

A Biblical Rough Draft

By Bob Odenkirk

FICTION

"God's

By Tipha

Boback flew to LifeLock's headquarters, in Arizona, and the executives he met were so enthusiastic that they called in the C.E.O., Todd Davis. Boback's pitch, Davis told me, had "great sizzle." Soon, a trial arrangement was negotiated. LifeLock turned over private information belonging to thirty thousand clients, so that Boback's team could demonstrate how Tiversa would protect them. Wallace later told the F.B.I. that, on Boback's instructions, he created about a hundred cases of false spread for those clients—manufacturing threats for people who had apparently experienced no data breaches whatsoever. According to Wallace, Boback used the LifeLock information to fill out passport applications and other official documents, which were uploaded to the Data Store, to give the impression that criminals had been circling Davis's customers. (Boback denies doing this.)

In January, 2009, Davis flew Boback to a desert resort in Phoenix, where he indicated over a long breakfast that he was ready to work together more closely. Boback returned home energized, and in the coming months he urged Davis to buy Tiversa. He proposed a price of more than a hundred million dollars, and then worked to demonstrate his company's value. "Every time we talked to him, he mentioned this *unbelievable* discovery that they had made," Davis recalled. "He was basically saving the world every few weeks."

month after Boback's breakfast with Davis, an NBC affiliate in Pittsburgh aired an explosive story: it reported that Tiversa, surveilling a computer in Iran, had discovered records involving one of the President's helicopters—part of a squadron known as Marine One. The origins of the story went back two years, to when Wallace joined the company. During one of his open-ended searches, he discovered files belonging to Vyalex Management Solutions, an avionics firm in Maryland, which served as a contractor for Naval Air Systems Command. Concerned that the breach might harm the military, he notified an Army officer who specialized in computer crime.

In February, 2008, the officer reached out to Vyalex's founder, an engineer named Al Leandre, to say that his company was exposing more than two hundred files. Leandre was horrified. When he was a boy, his family had fled Haiti's dictatorship for the U.S. As a young man, he had joined the Army, out of gratitude to his adopted home, and had worked on the electronic-warfare systems of the F-18. Although Vyalex was a private company, he regarded it as an extension of his service.

Leandre quickly discovered the source of the leak: a disused Vyalex laptop that his daughter had borrowed and used to run LimeWire. None of the files were classified, but he made a risk assessment of each one, and his team tried to determine whether the files had spread. Based on information that the officer provided, they found that three inconsequential business records, including one with "Amex" in its name, had ended up at an I.P. address in Tehran. But the address had no history of espionage; it apparently belonged to a civilian trawling for financial data.

Leandre purged the old laptop and provided the military with two detailed reports. He believed that the matter was resolved. But, several months later, Boback reached out, claiming that Tiversa was still detecting "very sensitive information from Vyalex." Rather than specify what kind of information, Boback directed Leandre to the *Post* story about Stephen Breyer, and warned that the reporter was "actively scouring the file-sharing networks to find any information relevant to 'DC-area businesses.' " He added, "For clarity, we would *never* provide any information or files to any reporter whether you decided to work with our firm or not, however he will probably find them."

Leandre politely told Boback that he had taken care of the breach, and could not afford the service. The next day, Boback wrote again, claiming that malicious people were scouring peer-to-peer networks *explicitly* for Vyalex records. "A great cause for concern," he said—adding that Tiversa could reduce its fee. "We can begin right away," he said. "Timing is critical to avoid the additional spread of the files."

Leandre told himself, "It sounds like blackmail." Again, he declined.

Half a year passed. Then, shortly after Boback had breakfast with Todd Davis, Tiversa began to advertise the Vyalex leak—in particular, a cost assessment that the Navy had given contractors, seeking bids to upgrade the electronic defenses of one of the President's helicopters. In a presentation to a firm that conducts business research, Tiversa noted that the file had been downloaded in Tehran. Wallace says that the claim sent him racing to the Data Store, where he appended the file about the helicopter to the same Iranian I.P. address that had downloaded the inconsequential Vyalex files.

Boback had assured Leandre that he would never publicize his misfortune, but two days later he gave an interview to NBC, noting that a defense contractor in Bethesda had exposed "highly sensitive blueprints for Marine One" that were later downloaded in Iran. (There were no blueprints.) Wesley Clark also spoke to NBC about the file. Trusting Boback's information—he says he knew of no impropriety at the company—he declared, "We know where it came from, and we know where it went."

Rachel Maddow and Wolf Blitzer quickly followed with their own segments. On CNN, an analyst speculated that Iranian cyber warriors were waiting for the file, ready to pounce. (Why? "We have no idea.") Lawmakers clamored for action. As Leandre watched the story on CNN, he began to understand that the media storm was about *him*. "I was scratching my head, and I was, like, Wow, Tiversa is making up this story," he told me.

Within days, his office was packed with federal agents. "There was F.B.I., Secret Service, Naval Criminal Investigative Service, and they were all interviewing me, *so stern*," he told me. "They were saying, 'Do you have any reason to harm the President?' And I'm, like, 'What are you talking about?' They thought this could have been some kind of espionage!" The investigation lasted for weeks, before the military exonerated

Leandre. "I lost weight, I vomited for so many days," he said. "I mean, I thought I was getting shipped to Guantánamo."

After his NBC interview, Boback and several Tiversa employees had dinner at a family restaurant north of Pittsburgh. An attendee later told the F.B.I. that Boback laughed about how he had got away with the story, while one of his tablemates plugged his ears and said that he didn't want to hear it.

When I pressed Boback about his media blitz, he told me, "I have often wondered if Wallace did, in fact, find the file in Iran. To this day, I have no idea." N.C.I.S. never verified that the file was in Iran, either. But, in the course of the inquiry, two agents paid a call on Tiversa. They interviewed Wallace, who, fearful of losing his job—Boback had just dramatically fired an executive—confirmed Tiversa's account of the file. Boback, meanwhile, found a way to turn the inquiry to his advantage. That March, a LifeLock executive wrote, asking, "Did you get a ride on the President's copter for saving the day on that one?" Boback replied, "No ride on the helo yet but I have had meetings with NCIS on Thursday. I already met with DoD, USSS, FBI, and Defense Security Service over the breach. I am trying to set up a broader deal with military on ID theft as well using our access now. Do you see what we bring to the table????? :-)"

The following month, LifeLock agreed to incorporate Tiversa into its premium service. That summer, Todd Davis invited Boback to a Nascar event that LifeLock was sponsoring at the Chicagoland Raceway. "I remember walking in with Todd, and there were these pictures of him there that were fifty feet tall—tons of them in the grandstand," Boback told me. Davis let him ride in the pace car with the event's grand marshal, Jimmy Fallon. Later in the trip, Boback impulsively bought a Lamborghini, his boyhood dream car, and shipped it home to Pittsburgh.

The headquarters of the Federal Trade Commission occupy a monumental building on Pennsylvania Avenue, in Washington. When the structure was erected, during the Great Depression, Franklin Delano Roosevelt heralded the commission's mandate to apply "the golden rule" to the conduct of business. Originally founded to protect consumers from monopolistic behavior, the F.T.C. was by then working to guard against false advertising and other unfair practices. At the headquarters, a granite sculpture—a man taming a wild horse—acknowledges the difficulty of that task.

As the F.T.C. began to explore its role in the digital marketplace, it had no technologists on staff, and no court had affirmed its authority in cybersecurity. But it was clear that the reason for concern was growing. Among the problems were peer-to-peer networks. By 2004, consumers had downloaded file-sharing programs more than six hundred and forty million times. When Boback testified before Congress in 2007, he framed the concern in a way that fit with the F.T.C.'s mission of protecting consumers: file-sharing programs could cause corporations to expose clients' private data. If such a security failure amounted to an "unfair act" against consumers, the commission reasoned, then it could intervene.

After Boback's testimony, lawyers with the F.T.C. reached out to him, requesting that Tiversa turn over information on companies that had exposed private customer information, so that it could investigate. The lawyers explained that they were prepared to issue Tiversa a legal demand for the information. (Companies often turn over privileged customer data only if compelled.) Tiversa asked that it be sent instead to a shell company that would serve as a conduit—the Privacy Institute, which listed an address at Boback's uncle's house, in New Jersey. This would neuter the demand, but the F.T.C. agreed. Tiversa's Data Store by then contained more than five million breached documents, and the lawyers wanted access.

When the demand arrived, Boback asked his staff to draw up a list of companies that fit the criteria. (He claims that this was the extent of his involvement.) The job fell to Wallace, who says that Boback helped him compile a kind of roster of retribution. In August, the Privacy Institute sent the F.T.C. a spreadsheet of eighty-four companies that had suffered security failures. None were Tiversa clients; eleven had worked with Tiversa for a time and then stopped.

Boback understood that he could exploit this information. As the list was being drafted, he sent a note to Todd Davis, marked "KEEP THIS CONFIDENTIAL." In it, he boasted that he had an inside tip: the F.T.C. was investigating about a hundred companies that had exposed private consumer data. (He neglected to mention Tiversa's role in the inquiry.) That autumn, Boback plotted with LifeLock to pitch the affected businesses. He claimed that the companies collectively had exposed information for as many as seven hundred thousand people, each one a potential customer, and he promised Davis "a huge upswing in members."

One of the companies on the list was an AIDS clinic in Illinois, the Open Door Clinic, which had declined to hire Tiversa to fix a data breach. Three days after Boback promised Davis a surge in membership, he and Wallace began calling Open Door patients whose information had been exposed. "One guy I talked to said, 'How did you know I was H.I.V.-positive? I haven't even told my family yet!' " Wallace recalled. "And it was, like, 'Sorry, bud, you probably should talk to Open Door.' " (Boback told me that Tiversa never made the calls. When I noted that phone records unearthed by Congress indicated otherwise, he said that they were likely faked.) Tiversa's lawyer also reached out to the patients, and filed a class-action suit against the clinic, which was eventually settled.

After the F.T.C. made its investigation public, in February, 2010, Boback triumphantly declared that fourteen of the companies on the list had contacted him for help. Davis told me that his own company didn't sign up any clients. But by then Tiversa's deal with LifeLock was bringing in so much business that Boback mounted an L.E.D. ticker on a wall to track the gains. Joel Adams decided to buy five million dollars' worth of shares. Although none of the money went into the company, Boback assured his employees they were millionaires who just didn't know it yet.

Despite this windfall, Tiversa was facing a growing problem. The F.T.C., in its effort to protect consumer privacy, had been pressuring the designers of peer-to-peer applications to make their software less confusing. Newer iterations of LimeWire effectively shut down the mechanisms causing accidental breaches; then, in 2010, LimeWire itself was shut down by a court injunction, for mass copyright infringement. At the same time, Spotify and other streaming services were causing people to stop sharing files entirely. EagleVision X1 was pulling in less and less. By the end of 2010, Todd Davis was noticing. Eventually, after paying Tiversa about forty million dollars, LifeLock cut all its ties.

To compensate for the diminishing flow of files, Tiversa's developers recalibrated the software to pull down virtually everything it encountered. Meanwhile, Boback tried to devise malware that would trick people into exposing files; he told his reluctant developers that it was for the intelligence community. Wallace, according to his F.B.I. testimony, hunted for material in hacked records from Sony, Stratfor, and Adobe and uploaded it to the Data Store.

Sam Hopkins cashed out and left. Increasingly, Boback told people that he had little interest in running the company. Amid the crisis, his behavior seemed scattershot. In 2012, Tiversa bought a seven-story landmark building in downtown Pittsburgh: a grand headquarters, plus extra floors that could be rented out for income. Boback created a spinoff, Tiversa Media, hoping to somehow monetize pirated MP3s that the system pulled in. In an upbeat note to Wesley Clark, he wrote, "We have now acquired the largest music repository in the world. We have roughly 4x the music content of Apple's iTunes." Clark remembers telling him, "What are you going to do with that? Is it legal?"

Boback was also working with MetLife on an I.D.-protection deal, resembling the one with LifeLock. For the pitch, he had devised a dramatic flourish. He purchased the Social Security numbers of several MetLife executives, from a service that private investigators use, then flashed them on a slide during a presentation, implying that Tiversa had found them on peer-to-peer. Bill Wheeler, who was MetLife's president of the Americas, saw through the stunt, but decided to sign on anyway. Once under contract, Boback began urging MetLife executives to buy his company.

V. WAR

Tiversa's undoing began in the summer of 2013, with a YouTube video. Michael Daugherty, the owner of a cancer-screening lab in Atlanta, had posted it to publicize his memoir, "The Devil Inside the Beltway"—a reference to the F.T.C., which Daugherty believed was destroying his company, in a conspiracy that included Tiversa. The video had an urban-doom aesthetic, reminiscent of "Batman." Over a soundtrack of percussion and agitato strings, it opened with three title cards: "Government Funded Data Mining and Surveillance," "Psychological Warfare," and "Abusive Government Shakedown." The sequence ended with an explosion and a pair of eyes glaring through a draped American flag—the book's cover art.

In the video, Daugherty appeared beside a mural-size painting of George Washington, wearing a white oxford shirt and a dark blazer. In a flat Michigan accent, he asked, "What am I doing here?" Then he put a red plastic whistle in his mouth and blew. He explained that he had built his company, LabMD, into a successful business, until "suddenly one day the phone rings, and it's a guy named Robert Boback."

The call came in 2008, after a computer in Daugherty's billing department exposed documents through LimeWire. Rick Wallace downloaded one of them—a file containing the private information of more than nine thousand patients—and a Tiversa sales executive made an initial pitch. Then Boback took over, pursuing a FUD-centered strategy. He declined to provide details about the source of the breach unless Tiversa was hired, while suggesting that the risk was growing because people were "searching precisely for the exact file name." This struck Daugherty as preposterous: the file's name was "insuranceaging_6.05.071.pdf." Offended by Boback's manipulations, he told Tiversa to direct all further communications to his lawyer, and put the matter out of his mind.

Then, in January, 2010, an attorney with the F.T.C. sent a letter, announcing that LabMD was under investigation for breaching federal data-security law. "The letter's immensity shocked me," Daugherty wrote in his memoir. In eleven pages of legalistic prose, the F.T.C. demanded proof of compliance. Daugherty sent over thousands of pages of records, noting that he had obeyed medical-privacy laws and had closed the breach the moment he learned of it. "The F.T.C. was on my mind at all hours of the day," he wrote. "If I was up in the middle of the night to use the restroom, I thought of the F.T.C. If I drove down the road to work, I thought of the F.T.C."

Almost as soon as the investigation began, Daugherty wondered if Tiversa had been involved: the LabMD file at the center of the inquiry was the same one that Boback had obtained. Haunted by the idea of a connection, Daugherty began researching. Both of his parents had been police officers, and, he told me, "my whole life was marinated in investigators and prosecutors and lawyers." He found that Tiversa had provided LabMD's breached documents to an academic at Dartmouth, and that Boback had cited them in congressional testimony, in 2009. The idea that Boback was publicizing his misfortune ate at him. He told himself, "This means war."

Daugherty's lawyer sent Tiversa a list of questions, which Boback ignored. Getting answers from the F.T.C. was no easier, and Daugherty began to vent his frustration. He claimed, publicly, that Tiversa had engaged in "property theft" when it took the file. Tiversa's lawyers responded with a cease-and-desist letter, which argued that the file had spread on peer-to-peer and was available for anyone to take. "Tiversa is not a

'thief,' " they insisted, adding, "The F.T.C. investigation is a direct result of LabMD's security failings, and nothing more."

The legal warning did not deter Daugherty from writing his book, which accused Boback of being a con artist and his company of "mental abuse." Boback, irritated, wrote to an associate, "The problem is that he needs a face to his 'villain' and unfortunately (and incorrectly) chose me." Soon after Daugherty posted the promotional video, Tiversa sued him for defamation. At almost the same time, the F.T.C.—nearly four years after it launched its inquiry—sued Daugherty's company for failing to safeguard its data. Tiversa became involved in both cases, maintaining that it had originally downloaded the LabMD file from a computer, in San Diego, that appeared to belong to an identity thief.

At Tiversa, a former employee told me, Boback seemed intent on pursuing Daugherty, even though it brought no obvious benefit to the company: "It got very cultish. We had this very charismatic leader, who would call these meetings for the entire company and start rambling about how he was being persecuted, how he was going to win, how crazy Daugherty was."

As the fight intensified, Rick Wallace was spending less and less time in the ops room. Once Tiversa signed up companies like LifeLock and MetLife, his skills at uncovering eye-catching records were less relevant. Boback, instead, pushed him into the role of part-time superintendent—dealing with elevator breakdowns, burst pipes, and broken light bulbs. Eventually, Boback hired Wallace and his wife, Amy, to clean up a house that he was flipping: a ramshackle place occupied by feral cats, which had left it in a toxic, stomach-turning condition. They called it Catmandoo.

Wallace began drinking heavily and talking less to Boback. Nonetheless, he says, Boback called him in just before Tiversa issued Daugherty the cease-and-desist letter, asking him to make it appear as if the LabMD file had spread across the peer-to-peer network. Wallace was reluctant: he was conscious that he had pulled down the file from Daugherty's company, and had noted his findings in writing. Still, he complied, linking the file in the Data Store to several burnt I.P. addresses. In 2013, as Tiversa pressed Daugherty to settle, he did so again, making it appear as if the file had spread to six locations, including a computer in San Diego.

Recognizing that his fabrications were becoming legally significant, Wallace began to come apart. "I was already stressed," he recalls—suffering, he says, from P.T.S.D., caused by his online research into child exploitation. On New Year's Eve, 2013, he got drunk and ended up in a physical altercation with his wife and daughter, and the police arrested him—the first of several arrests tied to drinking. "No one was even trying to understand what was happening to me," he told me. "I drank too much alcohol—always beer—and got in trouble."

In January, 2014, Wallace received a subpoena from Daugherty's lawyers, who were seeking to understand how the LabMD file had been exposed. He worried that he would have to either lie under oath or implicate himself and risk retaliation. After he expressed his fears to Boback, he says, Boback summoned him to his office, where he was toying with a pistol: "He's, like, 'Well, Waldo, if you fuck with the bull, you get the horn.' " (Boback says that he had no weapon, and that he simply directed Wallace to tell the truth—which, he maintains, is that he never ordered anyone to create false spread.)

On February 4th, Tiversa's lawyers agreed to have Wallace deposed. Soon afterward, Wallace says, he got a prescription for Ambien, which he took after drinking, then got into his car and totalled it. The following day, he drove the family's other car to Tiversa, where he and Boback had another standoff over the deposition. (Boback says they never met at the office.) As Wallace left, he says, Boback followed him into the elevator. "We were on the seventh floor, and he pushed the sixth-floor button, and as soon as the elevator doors closed he slammed me against the wall," Wallace recalled. Boback commanded him, again, to lie in order to corroborate the company's version of events. When the elevator arrived at the sixth floor, he got off.

Afterward, Wallace sat in his car and drank beer for a while, trying to calm down. Finally, he started the engine. "I just went around the corner from Tiversa and sped as fast as I could into a light pole," he says. "I just wanted to end it."

He was arrested. Boback picked him up and drove him home, warning that if he didn't get treatment for his drinking he would be fired. Days later, Wallace checked himself into a facility, which Boback had chosen. Whatever the benefits of rehab, it would also serve to isolate Wallace—perhaps even make his deposition impossible. (Boback told his executive assistant to avoid contact, explaining, "He needs treatment, not friends

right now.") When Daugherty's lawyers tried to contact him, they were told that he was inaccessible for medical reasons.

Almost as soon as Wallace started rehab, Boback fired him. He then hired a private-investigation company, Inpax GPS, to dig into the Wallaces' background, and brought security professionals to Tiversa to conduct "self-defense training." Inpax GPS produced a threat assessment that blended verifiable facts with assertions that seemed to originate from Boback, for instance that Wallace exhibited "extreme jealousy and threatening behavior directed toward Tiversa's CEO." It described Wallace's run-ins with the law, including one from 2013. The previous summer, the Wallaces had hosted an eight-year-old girl from New York, through the Fresh Air Fund, and the girl's mother complained that Wallace had behaved inappropriately. Wallace strenuously denied the accusation. Following an investigation, the authorities declined to pursue a case, and an administrative judge who reviewed the evidence recommended that the complaint be expunged. But Boback knew of the inquiry, and details about it turned up in the Inpax GPS assessment. He then cited the report to associates, giving the impression that Wallace was a molester.

When Wallace came home from rehab, some of his law-enforcement contacts would no longer return his calls. He had no obvious way to turn his career around, and felt increasingly isolated. On the evening of April 2, 2014, he was sitting in front of his computer at home. On impulse, he began searching for Mike Daugherty's number. A few months earlier, Daugherty had announced that he could no longer stay in business; in a melancholy note to employees, he had written, "Our futures are full of unknown waters." Suddenly, Wallace felt compelled to confess.

That evening, Daugherty was at a Thai restaurant in Atlanta. He had arrived early, and was waiting for some friends, when his phone rang. He answered, and a man's voice he didn't recognize said, "Is this Mike Daugherty?"

"Yeah," Daugherty said.

"Do you know the name Tiversa?"

"Yeah," Daugherty said.

"Well, I know a guy who would be willing to talk to you about what really happened. Can you talk to him? Would you retaliate?"

"Can you tell me who the guy is?"

"It's Rick Wallace," the man said.

Daugherty said that he wanted to get his lawyer's advice, and hung up. The lawyer told him to call back immediately, but Daugherty didn't have the number: the caller's I.D. was masked. Twenty minutes later, the man phoned again. Daugherty ran to the parking lot to take the call. "O.K., yes," he said, hurriedly. "I can talk to him."

There was a pause. "Well," the man said, "*I'm* Rick." Wallace almost immediately started to cry. "I destroyed your company," he told Daugherty. "I did terrible things." He spoke a little about what he had done at Tiversa; LabMD, he explained, had been on the list that went to the F.T.C. Then he passed the phone to his wife, and to one of their daughters. "Everyone was wanting to apologize," Daugherty recalled. He assured Wallace that redemption was possible. He said, "Let's focus on fixing this."

Daugherty strove to help Wallace obtain legal immunity to testify in his F.T.C. hearing, and he put Wallace in touch with the House Committee on Oversight and Government Reform. Darrell Issa, the committee's chairman, believed that LabMD's case raised questions about the scope of the F.T.C.'s authority. Moreover, Boback had twice testified before his committee. If he had not been truthful, Issa wanted to know. The committee launched an investigation.

Wallace was suddenly poised to be a star witness in two significant Washington inquiries. But he was drinking again, and still terrified of retaliation. In April, a congressional staffer reached out, to inform him that his testimony was required. Days later, he walked into the local police department in a panic, fearing that a scheduled call with Congress was a ruse orchestrated by Boback to intimidate him, or to find out what he planned to say. Wallace told the police that he had been receiving threatening phone calls and death threats posted on his car. His preoccupation with being harassed often interfered with his ability to testify. He later told congressional investigators that he found a Tiversa envelope in a shed behind his house, with a note scrawled on it:

"I.C.U." He took a photo—evidence, he said, that Boback was monitoring him and his family.

That spring, Boback travelled with his family to the Yemeni island of Socotra, and in the summer they went to Namibia. At home, though, he resembled a man at war. He hired the former White House press secretary Ari Fleischer to advise him in Washington, and he worked to assail Wallace's credibility with Congress and the F.T.C. Tiversa also passed the Inpax GPS threat assessment to David Sitler, the police chief in Wallace's community, who initiated a "force protection" measure. As summer gave way to fall, Wallace says, Sitler became a near-constant presence at his home. (Sitler, who was later fired for police brutality, denies this, saying, "We only monitored him if we came into contact with him.")

Inpax GPS also increased its efforts, assigning two investigators to track Wallace's movements. Under Boback's direct guidance, they coördinated with the police to place a hidden camera in a traffic cone outside Wallace's home. The footage was unremarkable—the mailman, Wallace's children—and after three days the investigators suggested that the surveillance be discontinued. An employee at Tiversa learned about the camera and secretly sent word to Wallace to be careful.

In November, 2014, the Department of Justice finally granted Wallace immunity to testify. Boback passed the news to one of his private investigators, striking a cool tone. "It will work out for the best," he told him. "Even though he will say ridiculous lies about Tiversa, he will get exposed." But, at the office, he seemed far from calm. Two former employees say that they witnessed Boback trying to manipulate Daugherty's file in the Data Store—making further changes to metadata that might figure in Wallace's testimony. In April, 2015, a month before the F.T.C. hearing, Wallace says, he found a warning chalked on his driveway: "U R DEAD."

Wallace was a quiet presence in court. Sitting before an administrative-law judge, he described systematically creating fraudulent file spread in the Data Store at Boback's direction. When asked how many Tiversa clients had been given false information, he said, "Probably every company that we've ever done business with." During testimony about Daugherty's company, the judge asked, "Did Mr. Boback have any reaction to LabMD's decision not to do business with Tiversa?"

"Yes," Wallace said.

"And what was that reaction?"

Wallace glanced at his lawyer, who instructed him to answer. "He basically said, Fuck him," he said. "Make sure he's at the top of the list."

The hearing triggered a storm of coverage—as Ari Fleischer informed Boback, "one story after another with similar bad headlines." CNN went with "Whistleblower accuses cybersecurity company of extorting clients." The bad press worsened after Darrell Issa's committee released a long report that asked whether Tiversa was a "hi-tech protection racket."

Joel Adams wrote to Boback, "F these guys Bob. We are the winners here." Boback responded, "They'll get theirs." With Fleischer, he drafted a letter to the *Wall Street Journal* saying that his company was a "good Samaritan." He argued that if Tiversa had never contacted LabMD its internal records would still be online, exposing the private information of thousands of patients. And he asserted that "the suggestion that Tiversa provided information on exposed files to the Federal Trade Commission as a means of retribution because LabMD didn't hire Tiversa is 100% false." Wallace, Boback said, "is an individual with a history of not telling the truth, and the information he testified about is demonstrably false." But he refrained from demonstrating how any of the allegations were false.

By this time, the Department of Justice had launched a criminal probe into Tiversa, and on March 1, 2016, a convoy of black vehicles filled with armed federal agents pulled up to the company's headquarters. They stormed the building and also interviewed employees at their homes, including one executive who was so nervous that he kept trying to drink from an empty water glass; eventually, he confessed to knowing that Wallace had added false metadata to the Data Store. The agents also commandeered records and seized the Data Store. The archive—a room filled with servers, stacked in racks seven feet tall—by then contained an estimated billion files, a trove measurable in petabytes. The federal agents sought to copy just a fraction of it; the process took so long that they needed a second search warrant.

Law-enforcement officers strive to keep such investigations secret. But, during the raid, a mysterious Twitter account made this impossible. By then, Tiversa's employees were in open revolt. (Several had left the company, while others had written to Adams, begging him to take action against Boback: "He risks everything for his own personal gain, and will lie to anyone to maintain his status.") The Twitter account posted a dramatic photo of the F.B.I. convoy, copying it to the Pittsburgh *Post-Gazette*, with a note indicating that Tiversa was being raided. The news was a deathblow. The board, driven by Adams, installed a new C.E.O., but there was very little that he could do. The company's brand was demolished. Tiversa would soon have to be sold.

The judge in Daugherty's case found Wallace credible, and he ruled against the F.T.C. (Based on a videotaped deposition, he deemed Boback evasive and untrustworthy.) His ruling was validated last year by an appellate-court judge, who noted, with unusual indignation, that the "aroma that comes out of the investigation of this case is that Tiversa was shaking down private industry with the help of the F.T.C." The commission's lawyer conceded, "Tiversa engaged in serious, serious misconduct." Before he could argue that the F.T.C. was untouched by that conduct, the judge cut him off, insisting that the commission should have let the matter go "after the evidence collapsed."

By then, Tiversa had been dismantled. It had too many liabilities to be sold outright, so the board had decided to carve out its assets. Still, no sale could be undertaken without ethical complications. The Data Store was the cybersecurity equivalent of nuclear waste—a vast repository of personal, financial, and corporate information, sensitive government records, and whatever else had been exposed on the Deep Web. Was it moral to put a price tag on it—to profit from, say, Justice Breyer's Social Security number? Was it even legal? Would there be an audit to insure that the deal contained none of the hacked content that Wallace had uploaded, none of the pirated music, no child pornography? The sale included health-care information protected by strict privacy laws. Was *that* a crime?

In February, 2017, Tiversa's primary shareholders began negotiations with Kroll, the corporate-intelligence firm, to sell off the company's core assets for several million dollars. The deal, closed within four months, was kept quiet. Earlier this year, a spokesperson for Kroll agreed to make an executive available to discuss the acquisition,

if I provided a list of questions in advance. After I sent the list, the discussion was abruptly cancelled. Kroll instead offered a brief statement. It said that Tiversa's technology strengthens its "existing business offerings," and that Kroll is not pursuing the company's former "business operations." One person involved told me that Kroll wanted the assets for corporate-intelligence purposes. It hired a handful of Tiversa employees to maintain the system. This January, someone in England detected it working and wrote on Twitter, "Care to tell me why you are snooping my I.P. address?"

After the raid on Tiversa, Boback moved his family to a waterfront compound in Florida, with a tennis court, a pool, a pier. He bought a construction company in Tampa Bay. Its Facebook page posted a photo of him, standing on a yellow Komatsu truck, wearing jeans and a safety vest and grinning.

At the time of the photo, Boback was still under federal criminal investigation. A year after the raid, though, the Department of Justice decided to drop its inquiry. Prosecutors typically do not comment on such matters, but it is possible to speculate on the reasoning. For one thing, the Data Store was a forensic hall of mirrors. For another, not all forms of FUD are criminal. Tiversa's actions never seemed to achieve the sharp edges of extortion. As for fraud, while some potential clients appear to have been fed entirely fabricated information, the tactic, as Wallace described it, was more often to exaggerate real breaches. It wouldn't be easy for a jury to delineate where Tiversa profited from fiction and where from fact. And, even though there were at least three other witnesses to the creation of false spread, the prosecution would have to build its case around the testimony of a man with a drinking problem and a record of arrests.

In March, 2017, two weeks before the Department of Justice closed its Tiversa case, Wallace fell from a tree while helping a neighbor do some pruning. He smashed his spine, and, paralyzed from the waist down, was unlikely to be able to testify for many months. Confined to a wheelchair, he now works as a security consultant. Daugherty is trying to return to health care. In the meantime, he promotes himself as an expert in "cybersecurity response," and focusses on litigation. He recently sent me a pie chart demonstrating the many cases he had initiated.

Boback, despite his efforts to project the image of a carefree construction magnate, remains mired in the legal fights over Tiversa, and is still sensitive to accusations about how he ran the company. Shortly after Joel Adams forced him out, he wrote a post on

LinkedIn promoting a memoir. When I asked about the book, Boback told me that it existed only in his mind—a fiction to communicate to business associates that he had a story to tell. In any case, he said, an imaginary memoir is the best kind to have when you can still be deposed.

The LinkedIn post described the book as the tale of a heroic businessman, fighting to overcome small-minded enemies—particularly Adams, whom Boback now likes to depict as the cause of Tiversa's problems. Titled "Politics of Greed," it would contain supportive forewords by Wesley Clark and Ari Fleischer. Although the book was still unwritten, Boback offered a sample of the advance buzz: a blurb from a reader who called his story a "travesty of justice," and one from another who asked, presumably of Adams, "Is this Pittsburgh's Bernie Madoff?" The description suggested that Boback was a whistle-blower, sacrificing everything to expose wrongdoing. "The entrepreneur was terminated, investigated, and 'scape-goated' in his effort to bring this information," it read. "However, he overcame these attacks to build a new multi-million dollar firm to provide the resources to bring this forward." Boback assured readers that he would ultimately triumph over his foes: "You'll be cheering in the end!" ♦

An earlier version of this article misstated the month of Richard Wallace's injury.

Published in the print edition of the November 4, 2019, issue, with the headline "The Burn List."

Raffi Khatchadourian became a staff writer at The New Yorker in 2008. *Read more »*