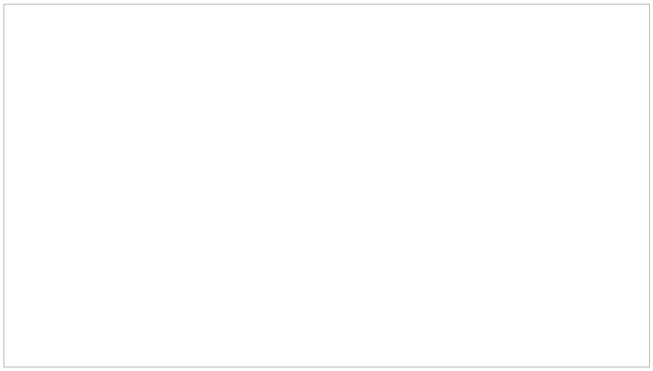
'-Who watches the watchers? Big Data goes unchecked

Wed, 14 May 2014 17:00:00, newstips66, [post_tag: big-data, category: elon-musk, category: google-alphabet, post_tag: google-big-data, post_tag: google-privacy-issues, category: idea-theft, category: worldnews]

Who watches the watchers? Big Data goes unchecked



Companies that see big profits in big data are pushing back against a crackdown. | AP Photo

By JOSH GERSTEIN and STEPHANIE SIMON | 5/14/14 5:01 AM EDT Updated: 5/14/14 6:40 PM EDT

The National Security Agency might be tracking your phone calls. But private industry is prying far more deeply into your life.

Commercial data brokers know if you have diabetes. Your electric company can see what time you come home at night. And tracking companies can tell where you go on weekends by snapping photos of your car's license plate and cataloging your movements.

Continue Reading

Private companies already collect, mine and sell as many as 75,000 individual data points on each consumer, according to a Senate report. And they're poised to scoop up volumes more, as technology unleashes a huge wave of connected devices — from sneaker insoles to baby onesies to cars and refrigerators — that quietly track, log and analyze our every move.

(Full coverage: Beyond the NSA series)

Congress and the administration have moved to rein in the National Security Agency in the year since Edward Snowden disclosed widespread government spying. But Washington has largely given private-sector data collection a free pass. The result: a widening gap in oversight as private data mining races ahead. Companies are able to scoop up ever more information — and exploit it with ever greater sophistication — yet a POLITICO review has found deep reluctance in D.C. to exercise legislative, regulatory or executive power to curb the big business of corporate cybersnooping.

The inertia — and lack of a serious legislative push — on private-sector data mining has several causes. Many Republicans are averse to any new regulation of business. Many Democrats are skittish about alienating campaign donors in Silicon Valley.

It's been more than two years since President Barack Obama announced — after two years of deliberation — that he would push for a Consumer Privacy Bill of Rights. Since then, no legislation has been introduced to implement it, and no regulations have been crafted. White House officials now acknowledge the proposal is outdated and may have been so on the day it was introduced.

Earlier this month, the White House again raised warnings about the erosion of personal privacy, with a report that clearly delineated the risks, as well as the promise, of the big data revolution — before calling for still more study.

Polls suggest that Americans want more protections. A national survey by Pew Research last fall found two-thirds of Internet users said current laws weren't adequate to protect consumer privacy online.

(Launching today: POLITICO Pro Cybersecurity)

But far from cracking down, the administration has floated several proposals for using data mining to advance its goals. The Pentagon, for instance, is considering tapping into commercial data banks to monitor the behavior of employees and contractors with top security clearances, so it can keep an eye out for bankruptcies, domestic violence charges or other signs of instability.

Senate Commerce Committee Chairman Jay Rockefeller (D-W.Va.), who has introduced legislation to rein in private data brokers, sounds resigned to the Internet remaining a kind of free-for-all for cybersnooping.

"Once we decided we're going with the Internet, we gave up our privacy," he said in an interview. "It's always the double side: It's the greatest discovery ever made and also one of the worst things that ever happened."

Asked if he sees a disconnect between the intense focus on NSA surveillance and the hands-off approach to private-sector data mining, Rockefeller responded: “You better believe it.”

(Also on POLITICO: 'Big data' review spotlights privacy)

Companies that see big profits in big data are pushing back against any talk of a crackdown. Their mantra: Regulation could stifle innovation.

“This is a situation in which technology, new data uses and new approaches are occurring and evolving very rapidly, and so if parameters were engraved in legislative stone, it could easily be the wrong measure, the wrong safeguards … and may very well inhibit the development of useful and socially desirable businesses and technology,” said Alan Raul, a lawyer for technology companies and a former member of George W. Bush’s White House privacy board.

Some tech titans have also tried to point a finger back at government, pushing for the administration to focus on reining in the NSA. Facebook founder Mark Zuckerberg, for instance, personally lobbied Obama to curb the NSA after allegations surfaced that the agency may have used social media services to deliver computer viruses that helped it conduct surveillance.

(CHECK OUT: 20 great quotes on NSA spying)

“I’ve called President Obama to express my frustration over the damage the government is creating for all of our future,” Zuckerberg wrote on his Facebook page in March. The government, he wrote, must be “much more transparent about what they’re doing, or otherwise people will believe the worst.”

‘IT’S KIND OF CREEPY’

The technological advances and cheap data storage have created surveillance opportunities that make logging phone calls look downright quaint.

At the mall, the corner store or the casino, hidden cameras may be snapping photos of your face and relaying them to companies that identify you, note your habits and trace your movements.

(Also on POLITICO: New NSA chief says agency has lost trust)

At home, smart meters can tell whether you have a plasma TV and what time you cook dinner. (Or even, perhaps, whether you’re growing marijuana in the basement.)

If you take more conventional prescription drugs, your pill bottles may soon email your doctor to let him know if you’ve been taking your medication.

Your car may let your mechanic know that your tires need rotating.

Your TV’s set-top box may soon be able to sense what you’re doing while you’re watching a show — snacking? snuggling? mopping? — and broadcast ads appropriate to the situation.

At school, your child’s online textbooks may be tracking his every click to understand how his brain works. Some publishers boast that they can tell when a student is on the verge of forgetting, say, how to multiply fractions — and can then send him a lesson custom-tailored to his learning style to fix that skill permanently in his memory.

Rep. Jason Chaffetz (R-Utah), who has fought NSA surveillance and is pushing a bill to limit government use of GPS-type data, seemed surprised when told by POLITICO about how much information on individuals is held in commercial databases.

“It’s kind of creepy,” he said. “People have a reasonable expectation of privacy from not only their government but from other individuals as well.”

In talking up big data, companies tout innovations they say will make the world safer, more convenient and more efficient. Automobile companies, for instance, are developing “connected cars” able to communicate with one another — and with stop signs and traffic lights and even nearby pedestrians — in hopes of making driving far less risky.

From a consumer perspective, the possibilities are almost endless. It could be quite handy to have a refrigerator that notes when the milk is expiring and automatically orders more. Some women might love a bra that senses emotions and texts them when stress levels rise.

By 2020, there could be more than 30 billion wireless devices connected to the Internet worldwide, according to ABI Research.

The trade-off: The more data these gadgets collect, the more intimate details they can expose.

“Are they going to be little snitches in our pockets, or are they going to be under our control and serving us?” asked Jay Stanley, a senior policy analyst with the American Civil Liberties Union.

Privacy advocates fear all this information will find its way to the commercial data brokers who compile and sell profiles packed with details about individuals’ health, behavior, interests and preoccupations, including education level, political and religious affiliations, and address, phone numbers and email accounts.

Some data brokers slice and dice consumer profiles into categories such as “Ethnic Second-City Strugglers,” “X-tra Needy” and “Fragile Families” for ease of marketing, the Senate Commerce Committee reported last year. One company sold lists of families afflicted by specific illnesses, from AIDS to gonorrhea — and even offered a specialty list of rape victims, until a reporter from The Wall Street Journal inquired about it.

It’s information that privacy advocates fear could be used to discriminate against individuals — or to target them with advertising cleverly designed to exploit vulnerabilities.

“We cannot even conceive of the ways our data is collected and then used to manipulate us at our weakest moments,” said Danielle Citron, a law professor and privacy scholar at the University of Maryland.

The industry responds that such concerns are overhyped.

Jennifer Glasgow, chief privacy officer for the data broker Acxiom, said the industry provides a valuable service by helping companies target their marketing more precisely. She said her company does not collect sensitive health information and sticks mainly to broad categories: Do you like golf? Do you drive a sports car or a minivan? What’s your ballpark income?

“Ferrari doesn’t want to bring people into the dealership for a free toaster oven if they’re in the $30,000 to $50,000 a year income range,” she said.

Acxiom launched a website last fall that lets consumers see their data files. About 250,000 have logged in to look, she said — and only 2 percent have opted to scrub their files from the system. About 20 percent have taken the time to correct the file, which suggests to Glasgow that they like having their information available to marketers.

“If you read a lot of the scare stories about data brokers … and then look at the site, you’ll be pleasantly underwhelmed,” Glasgow said. “You’re going to say, ‘That’s pretty accurate. It doesn’t scare me that they know about that.’”

SLOW GOING IN WASHINGTON

States have started to move on privacy protections, with a dozen passing laws in the past two years meant to safeguard citizens.

Utah has tried to put limits on the storage of license plate data captured by a growing network of cameras. California requires companies to make clear whether they honor the “do not track” signals on some web browsers. And a dozen states, including New Jersey, Colorado and Illinois, ban employers or schools from demanding access to social media accounts held by workers or students.

State attorneys general have also made several moves to police tech companies’ privacy practices. Among the most notable: a 38-state, $7 million settlement with Google last year over the company’s since-abandoned practice of having cars taking pictures for its Street View service also identify and capture data from nearby Wi-Fi networks.

In Washington, by contrast, things are moving at dial-up speed.

Continue Reading

Congress has been unable for years to write any serious privacy legislation. What little there is has fallen victim to partisan bickering, a slew of tech company lobbying and conservative interests fighting any form of regulation over the private sector’s use of data.

In his first term, Obama launched a series of discussions through the Commerce Department that led to the proposed Consumer Privacy Bill of Rights, a set of six principles to guide companies when handling personal data, including respecting the context in which it was obtained and allowing individuals to correct erroneous information.

“American consumers can’t wait any longer for clear rules of the road that ensure their personal information is safe online,” Obama said in releasing the guidelines in February 2012.

But the White House never made a follow-up push with Congress. There was some potential for bipartisan collaboration; Sens. John Kerry (D-Mass.) and John McCain (R-Ariz.) had earlier worked together on a similar framework. But “the White House was unable to pick up where the story had left off,” said Marc Rotenberg, executive director of the Electronic Privacy Information Center. “Apparently, they could wait.”

In fact, even as Obama vowed to safeguard consumer privacy, the White House repeatedly portrayed the big data revolution as a modern-day gold rush that could improve lives, boost the economy and create good jobs.

“Big Data is a Big Deal,” blared a March 2012 White House blog post announcing a $200 million Big Data Research and Development Initiative. An accompanying 13-page handout made only a glancing mention of privacy, for health records.

Obama’s political campaign was diving deep into data analytics, too, famously mining consumer databanks, voter surveys and social media to identify likely voters and push them to the polls.

Only after Edward Snowden’s first disclosures about NSA spying did Obama seem intent on reviving the privacy issue. He said on a couple of occasions that he was determined to pair discussions of alleged NSA overreach with a debate about the broader world of data-gathering.

“The challenges to our privacy do not come from government alone,” Obama said in January. “Corporations of all shapes and sizes track what you buy, store and analyze our data and use it for commercial purposes.”

Obama also commissioned counselor John Podesta to spend 90 days studying how data mining has affected privacy in both the public and the private sector. Podesta declined to comment for this story, but one former White House official said the Podesta project was, in part, meant to placate pro-privacy administration aides who had hoped for a tougher crackdown on NSA snooping.

“What comes out as ‘the administration position’ is highly contended internally,” said the ex-official, who asked not to be named. “Part of the reason the whole big data study is happening is as a counterbalance to those who had a sense the NSA really went way, way over the line.”

The Podesta report issued earlier this month called on Congress to take action now to crack down on data breaches, like the lapse that exposed the credit card numbers of tens of millions of Target customers over the holiday season. On privacy, though, the report recommended another round of discussion.

A handful of privacy bills are on the table in Congress, but none has made much headway. Among other things, the languishing bills would require companies to get customers’ permission before collecting or sharing information on their location; give consumers more control over the data collected by their cars; and expand online privacy protections for children.

McCain says legislation to control private-sector data collection would be a tougher lift than when he first proposed it three years ago. “It’s harder now, but one reason why we did it then and why it’s much more needed now is to try to give people some confidence in their ability to maintain their privacy,” he said.

Without a credible threat of legislative action, tech companies are unlikely to move voluntarily to tighten privacy protections, said Peter Swire, an adviser on privacy issues in both the Clinton and Obama administrations.

“Companies can justify expensive new privacy measures, if that’s better than potential legislation. [Otherwise,] it’s hard for them to self-impose strict privacy rules,” said Swire, who also served on Obama’s surveillance review group.

The Direct Marketing Association, an industry trade group, argues that industry self-regulation has worked well for decades. It’s also big business. The association released a study last fall estimating that the use of big data to shape marketing campaigns added $156 billion in revenue to the U.S. economy in 2012 alone.

The Rockefeller bill would give consumers the right to see and correct their files with data brokers or opt out of the system altogether. The DMA opposes the bill, said Rachel Nyswander Thomas, its vice president of government affairs. “It would very much impinge on this data-driven economy we’ve all come to enjoy,” she said.

PEN AND PHONE?

Regulatory agencies can sometimes be more nimble than Congress, and Obama has touted his desire to use his “pen and phone” executive branch power to get things done. But their actions in the privacy arena have also been sparse.

The Federal Trade Commission is way behind schedule on an analysis of commercial data brokers. And the agency is just starting to get up to speed on the universe of wired devices, known as the “Internet of Things.”

Instead of proposing regulation, the FTC is urging companies building connected devices to think carefully about data privacy as they’re developing their products.

“Risk to consumers could be minimized if companies would just give more serious thought to what data they really need and what they don’t,” said Jessica Rich, director of the FTC’s Bureau of Consumer Protection.

The FTC does have some enforcement power as well. In recent years, it has brought legal actions against dozens of organizations for violating consumer privacy rights. Most of those cases have flown under the radar, though the agency made headlines last week when it announced a settlement with the popular app Snapchat over concerns it misled users about the privacy of their communications.

As for the Consumer Privacy Bill of Rights, the White House’s outside tech advisers now believe that “ubiquitous” data collection may be rendering parts of it obsolete. With so many cameras, smartphones and new devices like Google Glass constantly collecting images, GPS location and other data, it no longer seems plausible that anyone can fully understand, let alone consent to, all the ways the flood of data about them is being used.

In a conference call with reporters earlier this month, Podesta said a “quick round of input” is needed on whether parts of the 2012 policy effort are still viable. “Some of the other elements of the Bill of Rights … may be under severe pressure in light of these new technologies,” Podesta said.

Indeed, even the concept of “consumer” privacy may now be off the mark. Back in 2012, the Obama administration focused largely on how companies treat data entered on a website or acquired during an online purchase. However, some of the trickiest policy challenges now stem from situations where the consumer is unaware of any transaction.

Privately owned license-plate readers capture the locations of millions of cars on public streets or shopping malls and upload that information to massive databases where it is for sale, with no government regulation.

Facial recognition software is approaching the same sophistication, creating the ability to build databases that could be used to track a person’s movements. Retailers, for instance, can use the technology to compare the faces of incoming customers to law enforcement mug shots. Or to flag VIP shoppers and text news of their approach to the store manager.

Some of those promoting and profiting from this technology believe they are protected by the First Amendment, since the courts have generally upheld the right to take and publish photos of scenes in public places. Utah ended up exempting the private sector from its rules on license plate data after two firms filed a lawsuit charging that the controls were unconstitutional.

”You have a recognized right to photograph anything that’s visible. To turn around and legislate how long you can retain those photos or with whom you may communicate that photography is clearly textbook First Amendment infringement,” said Todd Hodnett, chairman and founder of license plate tracking firm Digital Recognition Network. “I can’t imagine a world we would live in in which you get permission to photograph anything you can see with your eyes.”

The companies’ legal arguments might have some resonance with the current Supreme Court. But the Obama administration has also been quick to defend its right to regulate business in order to protect privacy.

Until the legal issues are resolved, private companies are likely to continue trying to find new ways to vacuum up every scrap of data they can find.

“The genius and the fury of capitalism is that everyone is trying to compete with each other about who can collect the most detailed information about consumers,” said Stanley, the ACLU policy analyst. “Where will it end? We have to put some rules in the road.”

Burgess Everett, Erin Mershon and Tony Romm contributed to this report.

Follow @politico

FOR MORE SEE HERE>>>