ONE NATION, TRACKED

Opinion | THE PRIVACY PROJECT

Total Surveillance Is Not What America Signed Up For

By The Editorial Board

DEC. 21, 2019

366

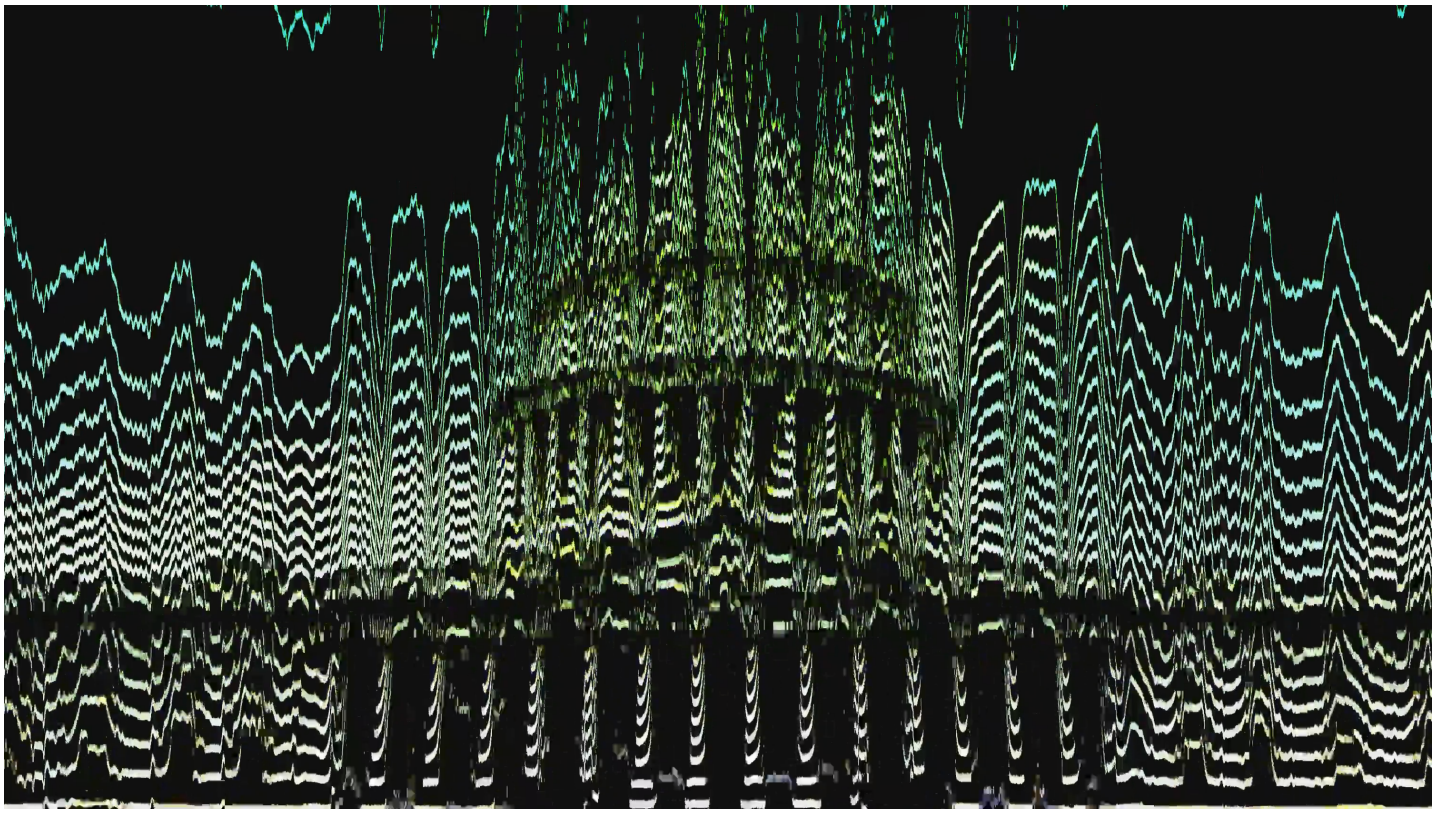

Illustration by Yoshi Sodeoka; Getty Images

IT IS A FEDERAL CRIME to open a piece of junk mail that's addressed to someone else. Listening to someone else's phone call without a court order can also be a federal crime.

The Supreme Court has ruled that the location data served up by mobile phones is also covered by constitutional protections. The government can't request it without a warrant.

But the private sector doesn't need a warrant to get hold of your data. There's little to prevent companies from tracking the precise movements of hundreds of millions of Americans and selling copies of that dataset to anyone who can pay the price.

The incongruity between the robust legal regime around legacy methods of privacy invasion and the paucity of regulation around more comprehensive and intrusive modern technologies has come into sharp relief in an investigation into the location data industry by Times Opinion. The investigation, which builds on work last year by The Times's newsroom, was based on a dataset provided to Times Opinion by sources alarmed by the power of the tracking industry. The largest such file known to have been examined by journalists, it reveals more than 50 billion location pings from the phones of more than 12 million Americans across several major cities.

By analyzing these pings, our journalists were able to track the movements of President Trump's Secret Service guards and of senior Pentagon officials. They could follow protesters to their homes and stalk high-school students across Los Angeles. In most cases, it was child's play for them to connect a supposedly anonymous data trail to a name and an address — to a real live human being.

Your smartphone can broadcast your exact location thousands of times per day, through hundreds of apps, instantaneously to dozens of different companies. Each of those companies has the power to follow individual mobile phones wherever they go, in near-real time.

That's not a glitch in the system. It is the system.

If the government ordered Americans to continuously provide such precise, real-time information about themselves, there would be a revolt. Members of Congress would trample one another to be first in front of the cable news cameras to quote the founders and insist on our rights to be free of such pervasive surveillance.

Yet, as a society, without ever focusing on this profound choice, we've reached a tacit consensus to hand this data over voluntarily, even though we don't really know who's getting it or what they're doing with it. As the close of 2019 approaches, everybody is searching for the meaning of the decade. Here's a thought: This is the decade — the period since the founding of the App Store, in 2008 — in which we were brainwashed into surveilling ourselves.

Related: From Adam Westbrook of The New York Times Opinion Video

Featuring NYT columnist Farhad Manjoo and contributing opinion writer Kara Swisher.

To be clear: The fact that Americans are tracked by the millions is not consumers' fault. There is no good-faith "opt out" when it comes to smartphone tracking. While there are steps that smartphone users can take to minimize the information gathered about their behavior, Americans who use surveillance devices like smartphones have only the illusion of control when it comes to protecting their privacy.

Location data collection is only one aspect of a surveillance economy that has sneaked into every corner of modern life. Tech companies have fostered a grass-roots surveillance culture that has convinced millions of Americans that they live better when they buy smart speakers, carry smart phones, watch smart televisions, turn their doorbells into unblinking video cameras.

There's no question that consumers, and society as a whole, receive many benefits from surrendering so much information, including better traffic mapping apps, more targeted advertisements and reviews of nearby restaurants. In the future, smarter artificial intelligence, safer self-driving cars and better medical care may also rely on location data. But there's no

reason that data needs to be gathered surreptitiously, stored forever in a manner that puts privacy at risk and allowed to be sold to the highest bidder.

The dangers inherent in today's smartphones and their near-universal adoption become obvious when you consider the enormity of the information being collected and how intimate it can be: a record of people visiting drug treatment centers, strip clubs, casinos, abortion clinics or other places where social stigma can create a powerful desire for privacy. The data we reviewed also reveals Americans making routine commutes from suburban homes to secret government facilities and making trips to churches and synagogues, to counseling sessions and chemotherapy treatments.

Given the far richer and more detailed data files available for pay, the dataset used in our series is comparatively tiny, a fleeting look under the curtain at the most expansive corporate surveillance advertising system ever constructed. It's all perfectly legal, largely unregulated and built to turn a profit.

As the protesters in Hong Kong who cut down high-tech lampposts to remove the threat of facial recognition cameras illustrate, uprooting a technology from society is far more difficult than regulating it before it achieves universal adoption. Location tracking through smartphones is already a reality for most Americans. But putting basic protections in place can still better protect the privacy of a nation of digital citizens while permitting innovation.

If the industry believes that data is a gold mine, Congress ought to force it to adopt practices to treat data in a manner commensurate with its value. That means increased security. It means rules clear and understandable to consumers about how it will be used. It means strict oversight of data collection, with penalties for deceiving consumers. It means further restrictions on collecting and monetizing the data of minors. It also means regulations that allow Americans to see where their data goes.

Some state and federal privacy laws apply to data that qualifies as "personally identifiable information," that is, information that could be used to identify a particular person, like full names, Social Security numbers and home addresses. Data classified as personally identifiable is subject to regulations that can restrict its distribution and sale, with penalties for violations.

Since there is no uniform federal definition of personally identifiable information, the states have created their own, with sometimes conflicting results. For instance, Massachusetts and California regard ZIP codes as personally identifiable, while other states do not. Federal lawmakers ought

to classify location data as personally identifiable. Several pieces of legislation have been introduced in Congress over the years that would do just this, though they haven't made it into law. But even the notion of personally identifiable information is becoming outdated since, as the Times Opinion investigation shows, so much can now be inferred from supposedly anonymous data.

So, as Congress considers federal privacy legislation, lawmakers could include measures to prevent the acquisition of location data if such collection isn't central to the function of the service. For instance, flashlight apps wouldn't be able to track location. A central principle of the General Data Protection Regulation, which governs privacy across the European Union, is "purpose limitation," meaning that data collected for one purpose cannot be used for another. The United States lacks such a protection — even California's new privacy law, which comes into force next year, doesn't have a purpose limitation provision.

Even in the absence of congressional action, regulators could be taking steps to better safeguard privacy. The Federal Trade Commission, for instance, could scrutinize data collection methods to see if they constitute deceptive practices under existing law.

The 1998 Children's Online Privacy Protection Act provides assurances that children under 13 will not be surveilled by websites and technology companies without their parents' permission. But it is difficult if not impossible for parents to understand the scope of the data being collected about their children and the stakes of having that information bought and sold. And why are the protections only for children under 13? In other ways, our laws recognize that teenagers up to 18 deserve special protections. Lawmakers should insist on regulations that prevent companies from surveilling the movement of all minors.

Freaked Out?
3 Steps to Protect Your Phone

Though studies show Americans are pleased by the convenience afforded by technological progress, many are either unsure or overwhelmed by the trade-off. If lawmakers don't act, we risk the further entrenchment of corporate surveillance in our lives.

It is time for Congress to hold technology and advertising companies accountable and make opting out of tracking a meaningful choice, if not the default setting. In a Capitol split by impeachment, the subject of privacy is a rare point of bipartisan concern, if not consensus.

“It doesn't have to be this way,” said Josh Hawley, a Republican senator from Missouri. “The reason it is this way is because the public is being actively misled by these tech companies when they tell the public that they can opt out. But the public can't opt out.” Mr. Hawley has introduced — and attracted Democratic co-sponsors for — do-not-track legislation that would block collection of data not central to the functioning of an online service or app.

“There is a Dickensian quality about this moment: the best and worst of times for this technology, which can enable and ennoble and degrade and debase,” said Edward Markey, a Democratic senator from Massachusetts. “For years, technology companies have talked about the enabling and ennobling. Now we’re starting to see the degrading and the debasement.”

What Times Opinion has been able to show in this series reflects just a tiny fraction of the data collected from the average American on any given day. The American public should see the full scope of the corporate surveillance to which it is subjected. Lawmakers have the power to subpoena companies and demand transparency about what data they collect from American citizens and what happens to it.

The price of participating in modern society cannot be turning our lives into open books, diaries of all travels and relationships and wants and desires to be read and passed along by corporations — corporations that are themselves not monitored or tracked in any meaningful way. Americans need to know how their information is being gathered, and whether it is being used to manipulate them. They deserve the freedom to choose a life without surveillance.

ONE NATION, TRACKED

AN INVESTIGATION INTO THE SMARTPHONE TRACKING INDUSTRY FROM TIMES OPINION

PART 1

WHAT WE FOUND

PART 2

PROTECT YOURSELF

PART 3

NATIONAL SECURITY

PART 4

HOW IT WORKS

HOW IT WORKS

PART 5

ONE NEIGHBORHOOD

PART 6

PROTESTS

Illustrations by Yoshi Sodeoka; Getty Images.