Your Right to Privacy

by Christopher Calabrese and Matthew Harwood via sal - ICH *Tuesday, Sep 24 2013, 10:57pm*
international / prose / post

> Among other eroded rights -- which YOU allowed to be stolen from under your noses -- privacy is now a thing of the past for the majority; but for those that wish to maintain anonymity and privacy be very cognisant of the words of evil Google chairman, Eric Schmidt, to paraphrase; "*if you want privacy today you have to FIGHT for it!*" Schmidt ALSO promised in an interview with Maddow on national television that he would never abuse his company's power. He promptly reneged on that promise after he was invited to attend the shadowy Bilderberg meetings!

Julian Assange also made a very quotable remark, "*smartphones are surveillance devices that also make calls!*" Have we got it now?

So there you have it, from both camps! So, keep using Google (ixquick is better) and spilling your guts on 'tracebook' and other social networking (info gathering sites) most of which were funded by the CIA, and continue making 'vanilla' open text calls and other unencrypted digital communications.

It really isn't too difficult to remain invisible -- our entire group has been doing it for decades; but to be sure, we use identity to hide our identities, very Zen!

Have you been told/reminded lately? You deserve everything you get from the criminal elites you allowed to reign over you -- you fuckin' mindless, cowardly, gullible, shameless slaves!

Story from ICH follows:

> **Destroying the Right to Be Left Alone**
>
> For at least the last six years, government agents have been exploiting an AT&T database filled with the records of billions of American phone calls from as far back as 1987. The rationale behind this dragnet intrusion, codenamed Hemisphere, is to find suspicious links between people with “burner” phones (prepaid mobile phones easy to buy, use, and quickly dispose of), which are popular with drug dealers. The secret information gleaned from this relationship with the telecommunications giant has been used to convict Americans of various crimes, all without the defendants or the courts having any idea how the feds stumbled upon them in the first place. The program is so secret, so powerful, and so alarming that agents “are instructed to never refer to Hemisphere in any official document,” according to a recently released government PowerPoint slide.
>
> You’re probably assuming that we’re talking about another blanket National Security Agency (NSA) surveillance program focused on the communications of innocent Americans, as revealed by the whistleblower Edward Snowden. We could be, but we’re not. We’re talking about a program of the Drug Enforcement Administration (DEA), a domestic law enforcement agency.

While in these last months the NSA has cast a long, dark shadow over American privacy, don't for a second imagine that it's the only government agency systematically and often secretly intruding on our lives. In fact, a remarkable traffic jam of local, state, and federal government authorities turn out to be exploiting technology to wriggle into the most intimate crevices of our lives, take notes, use them for their own purposes, or simply file them away for years on end.

"Technology in this world is moving faster than government or law can keep up," the CIA's Chief Technology Officer Gus Hunt told a tech conference in March. "It's moving faster I would argue than you can keep up: You should be asking the question of what are your rights and who owns your data."

Hunt's right. The American public and the legal system have been left in the dust when it comes to infringements and intrusions on privacy. In one way, however, he was undoubtedly being coy. After all, the government is an active, eager, and early adopter of intrusive technologies that make citizens' lives transparent on demand.

Increasingly, the relationship between Americans and their government has come to resemble a one-way mirror dividing an interrogation room. Its operatives and agents can see us whenever they want, while we can never quite be sure if there's someone on the other side of the glass watching and recording what we say or what we do -- and many within local, state, and federal government want to ensure that no one ever flicks on the light on their side of the glass.

So here's a beginner's guide to some of what's happening on the other side of that mirror.

You Won't Need a Warrant for That

Have no doubt: the Fourth Amendment is fast becoming an artifact of a paper-based world.

The core idea behind that amendment, which prohibits the government from "unreasonable searches and seizures," is that its representatives only get to invade people's private space -- their "persons, houses, papers, and effects" -- after it convinces a judge that they're up to no good. The technological advances of the last few decades have, however, seriously undermined this core constitutional protection against overzealous government agents, because more and more people don't store their private information in their homes or offices, but on company servers.

Consider email.

In a series of rulings from the 1970's, the Supreme Court created "the third-party doctrine." Simply stated, information shared with third parties like banks and doctors no longer enjoys protection under the Fourth Amendment. After all, the court reasoned, if you shared that information with someone else, you must not have meant to keep it private, right? But online almost everything is shared with third parties, particularly your private e-mail.

Back in 1986, Congress recognized that this was going to be a problem. In response, it passed the Electronic Communications Privacy Act (ECPA). That law was forward-

looking for its day, protecting the privacy of electronic communications transmitted by computer. Unfortunately, it hasn't aged well.

Nearly three decades ago, Congress couldn't decide if email was more like a letter or a phone call (that is, permanent or transitory), so it split the baby and decreed that communications which remain on a third party's server -- think Google -- for longer than 180 days are considered abandoned and lose any expectation of privacy. After six months are up, all the police have to do is issue an administrative subpoena -- a legal request a judge never sees -- demanding the emails it wants from the service provider, because under ECPA they're considered junk.

This made some sense back when people downloaded important emails to their home or office computers and deleted the rest since storage was expensive. If, at the time, the police had wanted to look at someone's email, a judge would have had to give them the okay to search the computer where the emails were stored.

Email doesn't work like that anymore. People's emails containing their most personal information now reside on company computers forever or, in geek speak, "in the cloud." As a result, the ECPA has become a dangerous anachronism. For instance, Google's email service, Gmail, is nearly a decade old. Under that law, without a judge's stamp of approval or the user ever knowing, the government can now demand from Google access to years of a Gmail user's correspondence, containing political rants, love letters, embarrassing personal details, sensitive financial and health records, and more.

And that shouldn't be acceptable now that email has become an intimate repository of information detailing who we are, what we believe, who we associate with, who we make love to, where we work, and where we pray. That's why commonsense legislative reforms to the ECPA, such as treating email like a piece of mail, are so necessary. Then the police would be held to the same standard electronically as in the paper-based world: prove to a judge that a suspect's email probably contains evidence of a crime or hands off.

Law enforcement, of course, remains opposed to any such changes for a reason as understandable as it is undemocratic: it makes investigators' jobs easier. There's no good reason why a letter sitting in a desk and an email stored on Google's servers don't deserve the same privacy protections, and law enforcement knows it, which is why fear-mongering is regularly called upon to stall such an easy fix to antiquated privacy laws.

As Department of Justice Associate Deputy Attorney General James Baker put it in April 2011, "Congress should also recognize that raising the standard for obtaining information under ECPA may substantially slow criminal and national security investigations." In other words, ECPA reform would do exactly what the Fourth Amendment intended: prevent police from unnecessarily intruding into our lives.

Nowhere to Hide

"You are aware of the fact that somebody can know where you are at all times, because you carry a mobile device, even if that mobile device is turned off," the CIA's Hunt explained to the audience at that tech conference. "You know this, I hope? Yes? Well, you should."

You have to hand it to Hunt; his talk wasn't your typical stale government presentation. At times, he sounded like Big Brother with a grin.

And it's true: the smartphone in your pocket is a tracking device that also happens to allow you to make calls, read email, and tweet. Several times every minute, your mobile phone lets your cell-phone provider know where you are, producing a detail-rich history of where you have been for months, if not years, on end. GPS-enabled applications do the same. Unfortunately, there's no way to tell for sure how long the companies hang onto such location data because they won't disclose that information.

We do know, however, that law enforcement regularly feasts on these meaty databases, easily obtaining a person's location history and other subscriber information. All that's needed to allow the police to know someone's whereabouts over an extended period is an officer's word to a judge that the records sought would aid an ongoing investigation. Judges overwhelmingly comply with such police requests, forcing companies to turn over their customers' location data. The reason behind this is a familiar one: law enforcement argues that the public has no reasonable expectation of privacy because location data is freely shared with service or app providers. Customers, the argument goes, have already waived their privacy rights by voluntarily choosing to use their mobile phone or app.

Police also use cell-phone signals and GPS-enabled devices to track people in real time. Not surprisingly, there is relatively little clarity about when police do this, thanks in part to purposeful obfuscation by the government. Since 2007, the Department of Justice has recommended that its U.S. attorneys get a warrant for real-time location tracking using GPS and cell signals transmitted by suspects' phones. But such "recommendations" aren't considered binding, so many U.S. Attorneys simply ignore them.

The Supreme Court has begun to weigh in but the issue is far from settled. In United States v. Jones, the justices ruled that, when officers attach a GPS tracking device to a car to monitor a suspect's movements, the police are indeed conducting a "search" under the Fourth Amendment. The court, however, stopped there, deciding not to rule on whether the use of tracking devices was unreasonable without a judge's say so.

In response to that incomplete ruling, the Justice Department drew up two post-Jones memos establishing guidelines for its agents and prosecutors regarding location-tracking technology. When the American Civil Liberties Union (ACLU) filed a Freedom of Information Act request for those guidelines, the Justice Department handed over all 111 pages, every one of them redacted -- an informational blackout.

The message couldn't be any clearer: the FBI doesn't believe Americans deserve to know when they can and cannot legally be tracked. Supreme Court Justice Sonia Sotomayor drove home what's at stake in her concurring decision in the Jones case. "Awareness that the Government may be watching chills associational and expressive freedoms," she wrote. "And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse... [and] may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"

The ability of police to secretly track people with little or no oversight is a power once only associated with odious police states overseas. Law enforcement agencies in the United States, however, do this regularly and enthusiastically, and they do their best as well to ensure that no barriers will be thrown in their way in the near future.

Sting(ray) Operations

During one of his last appearances before Congress as FBI director, Robert Mueller confirmed what many insiders already assumed. Asked by Senator Chuck Grassley whether the FBI operates drones domestically and for what purpose, Mueller responded, “Yes, and for surveillance.” This was a stunning revelation, particularly since most Americans associate drone use with robotic killing in distant lands.

And, Grassley followed up, had the FBI developed drone guidelines to ensure that American privacy was protected? The Bureau, Mueller replied, was in the beginning phase of developing them. Senator Dianne Feinstein, hardly a privacy hawk, seemed startled by the answer: “I think the greatest threat to the privacy of Americans is the drone, and the use of the drone, and the very few regulations that are on it today,” she said.

The senator shouldn’t have been shocked. The government’s adoption of new intrusive technologies without bothering to publicly explore their privacy implications -- or any safeguards that it might be advisable to put in place first -- isn’t an aberration. It’s standard practice. As a result, Americans are put in the position of secretly subsidizing their own surveillance with their tax dollars.

In July, for example, the ACLU published a report on the proliferating use of automatic license-plate readers by police departments and state agencies across the country. Mounted on patrol cars, bridges, and overpasses, the cameras for these readers capture the images of every license plate in view and run them against databases for license plates associated with stolen cars or cars used in a crime. Theoretically, when there’s a hit, police are alerted and someone bad goes to jail. The problems arise, however, when there’s no hit. Most police departments decide to hang onto those license-plate images anyway, creating yet another set of vast databases of innocent people’s location history that’s easy to abuse.

Since technology almost always outpaces the law, regulations on license plate readers are often lax or nonexistent. Rarely do police departments implement data-retention time limits so that the license plates of perfectly innocent people are purged from their systems. Nor do they set up rules to ensure that only authorized officers can query the database when there’s evidence that a particular license plate might be attached to a crime. Often there aren’t even rules to prevent the images from being widely shared with other government agencies or even private companies. These are, in other words, systems which give law enforcement another secret way to track people without judicial oversight and are ripe for privacy abuse.

As is often the case with security technology -- for instance, full-body scanners at airports -- there’s little evidence that license plate readers are worthwhile enough as crime fighting tools to compensate for their cost in privacy terms. Take Maryland. In the first five months of 2012, for every million license plates read in that state, there were just 2,000 “hits.” Of those 2,000, only 47 were potentially associated with serious crimes. The vast majority were for minor regulatory violations, such as a suspended or revoked vehicle registration.

And then there’s the Stingray, a device first used in our distant wars and so intrusive that the FBI has tried to keep it secret -- even from the courts. A Stingray mimics a cell-

phone tower, tricking all wireless devices in an area to connect to it instead of the real thing. Police can use it to track suspects in real time, even indoors, as well as nab the content of their communications. The Stingray is also indiscriminate. By fooling all wireless devices in an area into connecting to it, the government engages in what is obviously an unreasonable search and seizure of the wireless information of every person whose device gets caught up in the "sting."

And when the federal government isn't secretly using dragnet surveillance technologies, it's pushing them down to state and local governments through Department of Homeland Security (DHS) grants. The ACLU of Northern California has, for example, reported that DHS grant funds have been used by state and local police to subsidize or purchase automated license plate readers, whose images then flow into federal databases. Similarly, the city of San Diego has used such funds to buy a facial recognition system and DHS grants have been used to install local video surveillance systems statewide.

In July, Oakland accepted $2 million in federal funds to establish an around-the-clock "Domain Awareness Center," which will someday integrate existing surveillance cameras and thermal imaging devices at the Port of Oakland with the Oakland Police Department's surveillance cameras and license plate readers, as well as cameras owned by city public schools, the California Highway Patrol, and other outfits and institutions. Once completed, the system will leverage more than 1,000 camera feeds across the city.

Sometimes I Feel Like Somebody's Watching Me

What makes high-tech surveillance so pernicious is its silent, magical quality. Historically, when government agents invaded people's privacy they had to resort to the blunt instruments of force and violence, either torturing the body in the belief it could unlock the mind's secrets or kicking down doors to rifle through a target's personal effects and communications. The revolution in communications technology has made such intrusions look increasingly sloppy and obsolete. Why break a skull or kick down a door when you can read someone's search terms or web-surfing history?

In the eighteenth century, philosopher Jeremy Bentham conceived of a unique idea for a prison. He called it a "panopticon." It was to be a place where inmates would be constantly exposed to view without ever being able to see their wardens: a total surveillance prison. Today, creating an electronic version of Bentham's panopticon is an increasingly trivial technological task. Given the seductive possibilities now embedded in our world, only strong legal protections would prevent the government from feeling increasingly free to intrude on our lives.

If anything, though, our legal protections are weakening and privacy is being devalued, which means that Americans with a well-developed sense of self-preservation increasingly assume the possibility of surveillance and watch what they do online and elsewhere. Those who continue to value privacy in a big way may do things that seem a little off: put Post-it notes over their computer cameras, watch what they tweet or post on Facebook, or write their emails as if some omnipresent eye is reading over their shoulders. Increasingly, what once would have been considered paranoid seems prescient -- self-defense and commonsense all rolled into one.

It's hard to know just what the cumulative effect will be of a growing feeling that nothing is truly private anymore. Certainly, a transparent life has the potential to rob an

individual of the sense of security necessary for experimentation with new ideas and new identities without fear that you are being monitored for deviations from the norm. The inevitable result for many will be self-censorship with all its corrosive effects on the rights of free speech, expression, and association.

The Unknown Unknowns

Note that we've only begun a tour through the ways in which American privacy is currently under assault by our own government. Other examples abound. There is E-Verify's proposed giant "right-to-work" list of everyone eligible to work in the United States. There are law enforcement agencies that actively monitor social media sites like Facebook and Twitter. There are the Department of Homeland Security's research and development efforts to create cameras armed with almost omniscient facial recognition technology, not to speak of passports issued with radio frequency identification technology. There are networked surveillance camera feeds that flow into government systems. There is NSA surveillance data that's finding its way into domestic drug investigations, which is then hidden by the DEA from defense lawyers, prosecutors, and the courts to ensure the surveillance data stream continues unchallenged.

And here's the thing: this is only what we know about. As former Defense Secretary Donald Rumsfeld once put it, "there are also unknown unknowns -- there are things we do not know we don't know." It would be the height of naïveté to believe that government organizations across this country -- from the federal to the municipal level -- aren't engaged in other secret and shocking privacy intrusions that have yet to be revealed to us. If the last few months have taught us anything, it should be that we are in a world of unknown unknowns.

Today, government agencies act as if they deserve the benefit of the doubt as they secretly do things ripped from the pages of science-fiction novels. Once upon a time, that's not how things were to run in a land where people prized their right to be let alone and government of the people, by the people, and for the people was supposed to operate in the open. The government understands this perfectly well: Why else would its law enforcement agents and officers regularly go to remarkable lengths, sometimes at remarkable cost, to conceal their actions from the rest of us and the legal system that is supposed to oversee their acts? Which is why whistleblowers like Edward Snowden are so important: they mount the last line of defense when the powers-that-be get too accustomed to operating in the dark.

Without our very own Snowdens working in the county sheriff's departments or big city police departments or behemoth federal bureaucracies, especially with the world of newspapers capsizing, the unknowns are ever more likely to stay unknown, while what little privacy we have left vanishes.

*[Ok, I'll give you a hint -- today's **digital technology is a double-edged sword**, though the powers certainly do not wish that information to become widely known; they are using propaganda methods to frighten you into thinking they control that technology when REALITY DICTATES OTHERWISE. Indeed, the **evil powers use digital technology but hackers and the 33.333 underground are more 'proficient users!'** So you see, we have them by the balls and they have YOU by the balls, you*

pathetic, cringing cowards -- LOL! They are only a handful and you are BILLIONS; if you wish to restore Democracy and Privacy and other stolen rights, then DO IT!]

http://www.informationclearinghouse.info/article36329.htm
