Who cares that we no longer have privacy?

Ransom Stephens - September 26, 2017

They know where you are. They know where your car is parked. They know who you're with. They know your credit rating. If they don't already, they'll soon know your pulse rate, whether or not you're awake, and someday even your electro-encephalogram (EEG).

Whether or not you care probably depends on who has the information and how they'll use it. Pick your bogeyman—the government, huge corporations, your life/health/car insurance company, your bank, your spouse's private investigator—they can all get your information.

I leave my cell phone's GPS positioning turned off. Still, if I'm connected to WiFi or in a well-covered area, Verizon and those who hack it can triangulate base stations and isolate me to within a block. If I'm out in the sticks, the least they know is the time I was last near a base. In any case, they know where you've parked.

Police surveillance cameras all but cover the United Kingdom. There are far fewer in the US, but those deployed by companies and home owners make up the difference; most store entrances have them, every ATM machine has at least one, most public transportation has them (and some even function!).

Every person packs biometric signatures—fingerprints, retina, voice, scent, walking gait, and the ultimate: your connectome—and we're surrounded by devices with microphones and cameras that may or may not be active. Most microphones are active all the time, if only to catch their interrupt phrase—"Ok Google?," "Alexa?," "Hey Siri"—or at least that's what your-most-feared-bogeyman would have you believe, but they analyze every sound.

Always assume that you're being watched.

That sentence might send chills down your spine, especially if you're an old geezer who thinks that going incognito is the best way to go.

Last year, I wrote an article in this space that celebrated EDN's 60th birthday and I got a bunch of email because people were amused by the last few paragraphs. Set 60 years in the future, it described my experience trying to explain the concept of privacy to my great-great-great granddaughter: "She found it very difficult to get her head around the idea that you could be somewhere without other people knowing where you were or what you were doing. On the downside, her father, my great-great grandson, chewed me out for scaring her. She's having a recurring nightmare where she's walking along a beach and no one knows her opinion."

As IoT gadgetry proliferates, our privacy will decay further. Every time a new technology is introduced to society, it both solves problems and creates new problems. In our business, we call that job security.

Successful crimes require privacy, so one could argue that privacy is less valuable than safety, after all, "What are you hiding?" Surveillance cameras help police solve crimes and police officers who wear cameras receive far fewer complaints than those whose actions are not recorded.

Maybe my generation will be the last that values privacy. I'm not sure why I don't want others to know my actions, but I don't. I must be hiding something, right? Maybe I don't want you to know that occasionally I do things you don't want to know about. I'm hiding it as a matter of courtesy. Maybe you're guilty of these same crimes. Please don't tell me.

Identity recognition can be run in real time on vast quantities of video and audio data. The data can be sorted into places, times, associations with other people, proximity to crimes, and likelihoods that you have participated in a "crime." I put "crime" in quotes because whether or not an activity is a crime depends on the observer. For example, if you ticked the "no tobacco" box on your life-insurance application, then smoking is a crime to you—bang, your survivors get nothing because your insurance company found video of you firing up a stogie five years ago when your favorite team won the title. We face a potentially civilization-crippling problem as we enter the era of comprehensive surveillance.

If the information gathered is kept secret by corporations/government/your-most-feared-bogeymen, then that information can be selected and edited to present the bogeymen in a positive light, no matter how evil their actions, just as it can be used to present you in a negative light no matter how altruistic your actions.

Just one inalienable right stands between us and utter manipulation by the bogeyman: our right to look back at them. Unfortunately, in the last 20,000 years our inalienable rights have been more often denied than permitted.

Transparency is our only safeguard and we, the people who develop surveillance technology, are obligated to demand it! More on that next time.

—Ransom Stephens is a technologist, science writer, novelist, and *Raiders fan*, which explains why he hasn't fired up a cigar for quite some time.

Related articles:

- How to design an optical heart rate sensor into a wearable device’s wristband
- Handling Privacy and Security Concerns in the IoT: Protecting Data
- IoT Security: What We Need Next
- 5 Biggest IoT Security Blunders
- Standardizing the Internet of Things: Why Our Money Is on Bluetooth Smart