

How “Nothing to Hide” Leads to “Nowhere to Hide” – Why Privacy Matters in an Age of Tech Totalitarianism



by [TDB](#)

Editor’s note: The following comes from a longtime journalist who specializes in writing for major media outlets and private companies about robots, Big Data, and Artificial Intelligence (AI).

Would you allow a government official into your bedroom on your honeymoon? Or let your mother-in-law hear and record every conversation that takes place in your home or car – especially disagreements with your husband or wife? Would you let a stranger sit in on your children’s playdates so that he could better understand how to entice them with candy or a doll?

Guess what? If you bring your phone with you everywhere, or engage with a whole-house robo helper such as Alexa or Echo or Siri or Google, you’re opening up every aspect of your life to government officials, snooping (possibly criminal) hackers, and advertisers targeting you, your spouse and your children.

The following is not a screed against technology. But it is a plea to consider what we’re giving up when we hand over privacy, wholesale, to people whom we can neither see nor hear... people whose motives we cannot fathom.

The widened lanes of communication, and the conveniences that Smart Phones, wireless communities, Big Data and Artificial Intelligence (AI) have fomented are indeed helpful to some extent. They allow, for example, for remote working, which allows people to spend more time with their families and less time commuting. In areas such as the

energy business, the field of predictive analytics, born of Big Data and the Industrial Internet, helps mitigate the danger of sending humans to oil rigs at sea.

And on a personal level, of course, the conveniences are innumerable: Grandparents living far away can “see” their grandchildren more often than they could in years past, thanks to technology such as FaceTime and Skype.

People save money: As you walk by a restaurant, a lunch coupon suddenly appears on your phone.

And they can save time: Someday soon, the Internet of Things might tell your coffee maker and alarm clock to go off before its normal time, because bad weather is coming and your son’s school bus will arrive 15 minutes early to avoid the fog.

But there’s a corollary we must think about. (Two corollaries, actually, one being the long-term effects of Electromagnetic Fields on our health, and especially on our brains. But so far, few studies have been funded to examine this.)

We must acknowledge that we’re gaining all this convenience at the expense of our privacy.

When you ask Siri or Echo or Alexa or Google (and others of their ilk) something, it’s great to get an immediate answer... but the corollary is that Siri and Echo and Alexa and Google are listening to every conversation you’re having with your spouse, every fight you’re having with your kids, and every bit of heavy breathing that might be taking place in the dark.

That response inherently grants legitimacy to the search in the first place. The implication is that if you have nothing to “hide,” then the tech companies, the advertisers, the government, etc. should indeed have full access to every aspect of your life.

Note that the word in the phrase is “hide” and not “protect”, thereby implying that all that is not shared with any intrusive party must be something nefarious, something you’re trying to keep from those who have a right to it.

And if you think about it, “nothing” is the wrong word, too: Forgive the vulgarity here, but would you use the toilet in front of your mother-in-law? Would you allow an IRS official into your bedroom at night? Or to move into your home and record every conversation that takes place? Would you open your private diary to your spouse’s ex or to your children? Clearly, there are some things we do indeed wish to keep private.

In other words, if it’s OK to want to protect the privacy of one’s genitals or one’s private thoughts, why is it wrong to want to protect one’s conversations or whereabouts?

Totalitarianism and Tech - Caveat Emptor

Privacy is the first thing that a totalitarian state attempts to destroy.

Ask anyone who lived behind the Berlin Wall or in Stalinist Russia. If you know what parents are teaching their children, you can intervene and destroy the family, a primary goal of totalitarianism. If you know someone’s secrets or vulnerabilities, you can manipulate him.

Knowledge truly is power, especially if you are a big state wanting to control people.

As a child, I was a huge fan of figure skating, and in particular of the great, then-East German champion Katarina Witt. In an interview a few years ago, she revealed her shock that the Stasi collected thousands of records of all her comings and goings and private conversations. The spies even noted when she had been intimate with her boyfriend.

When the government knows all, no one is immune, and everyone can be controlled.

And just think, they were documenting Miss Witt's activities and conversations by hand, back in the 1970s and '80s. Now, nearly every single aspect of our lives is being recorded in real time. Every email, every text, every phone conversation. Every time you allow your phone to know where you are, your whereabouts are noted. Soon, that Internet of Things — IoT — which already connects 50 billion “things” through an internet of its own, will be coming to your refrigerator, your dishwasher, your coffeemaker. Happy Alexa and GE “smart fridge” commercials are airing as we speak.

And not only are we letting all of this happen, we're welcoming it. Twenty years ago, it was Miss Witt's friends who recorded her personal conversations, and strangers who spied on her. But as she has noted, these days, we give a lot of our privacy away of our own free will. If someone were parked outside your house, surveilling you day and night, it would be unnerving, no? But we're fine keeping our phones on us 24/7, and telling Facebook personal details about ourselves.

We do this because of the convenience, which will be increasing in scope as quickly as do the various surveillance mechanisms. Will it be convenient when your fridge tells your phone that you're running low on orange juice (as the bottle will have a sensor, too)? Perhaps.

But will it be convenient when that same fridge tells your health insurance company that you've got ice cream in the freezer? And when your rates go up because of it?

Worse - will it be convenient when that fridge listens to your kitchen conversations and tells the government that you'll be organizing a political discussion group on Tuesday? Or when it tells that bizarre man you went on one date with, who hacked your system, that your daughter has a recital this Friday night?

This is not a conspiracy theory. This is an extrapolation of what happens when people who crave power gain access to vast amounts of personal information.

The more you tell Facebook, or Siri, or Google, or FourSquare, or your phone, or your washing machine, then the more of your own personal power and privacy you're giving up. (And the more photos you post of your young children, the more of their power you're relinquishing. So, parents — stop. Now.)

Bottom line: Once the state (or a company) knows your weaknesses, they can exploit them. They can go after you in myriad ways. And I don't just mean to "punish" you... I mean to manipulate you.

If a politician has access to your personal proclivities, then he can easily craft, via Artificial Intelligence, a targeted campaign that caters to exactly what the data tell him you want to hear. In the future, he could even warp news stories, video and even audio in real time to appeal to you for gain.

If a potential employer is considering you for a job, then she can (already) access every YouTube video you've ever watched, every public post you've ever made, and, soon, everything else you've put online. In the future, she might be able to access everything you've ever said in your home or in your car, or every video of you taken by your television when you think it's off.

Those conversations and images will be sold as commodities. "Data" = "money" and "power." Companies will soon specialize in mining all that personal data; they'll be paid to flag "inappropriate" conversations, texts or images. Think about it.

A private banker I spoke to in Asia is proud of the fact that his bank is working in concert with FinTech to develop Know Your Customer technology on steroids: It will find every single email, text message, photo, post, and even online search that you've ever done so that it can (and this sounds so innocuous) "paint a holistic and predictive picture of client needs."

That predictive part is critical. Not only do data tell those who hold them where you've been, but AI and Big Data analysis can predict

where you're going (both physically and psychologically)... and here's the really scary part... before you know it.

That gives the data holders real powers of manipulation. The winners of a battle are nearly always the ones with the advanced information, the ones who can launch the surprise attack.

Technology can lead to convenience, but it can also lead to abuses of power. In its extreme, that is called totalitarianism.

In the end, we must take precautions if we're to have anything close to liberty. Some of you have, no doubt, read Jonah Goldberg's excellent book from 2007, *Liberal Fascism*, the hardcover of which features a smiley face graphic with a Hitler mustache. In the introduction, Mr. Goldberg quotes a segment from a Bill Maher show in which George Carlin says, in essence, (and I'm paraphrasing) that "when fascism comes to America it will be wearing a smiley face."

I'd go a step further — it will be cloaked in an emoji... seemingly innocuous, friendly, and ubiquitous.

We must stop giving away our privacy. We must start thinking about personal "data" as the commodity that it already is, and even as a weapon that can be used against us.

If we don't stop and reconsider what we're giving away, not only will there be nothing to hide, but *nowhere* to hide.