UNITARIAN UNIVERSALIST
CONGREGATION OF FREDERICK
Spirituality · Community · Justice

"Privacy, Social Justice, & Survival in a Hyper-connected World"

The Rev. Dr. J. Carl Gregg

25 November 2018

frederickuu.org

The late Alan Westin (1929 - 2013) was a Professor of Public Law & Government at Columbia University. In the late 1960s and early 1970s, he wrote two major books on privacy, and it is no coincidence that both book titles include the word *free*: *Privacy and Freedom* (1967) and *Databanks in a Free Society* (1972). Keep that word *freedom* in mind because it is more important than might be initially clear. Privacy is about more than what you do that no one knows about; **privacy is deeply a part of what is required to be a free people who are part of a free and open society.**

Dr. Westin's research is "widely seen as the first significant work on the problem of consumer data privacy and data protection…. His books prompted U.S. privacy legislation and helped launch global privacy movements in many democratic nations in the 1960s and 70s." Privacy, as we will see, is central to the liberal democratic tradition generally—and to our UU tradition in particular.

One classic definition of privacy is from the nineteenth-century British philosopher John Stuart Mill's (1806 - 1873) book *On Liberty*:

> the sole end for which [humankind is] warranted, individually or collectively in interfering with the liberty of action of any of their number is self-protection. That the only purpose for which power can be rightfully exercised over any member of a civilized community, against [their] will, is to prevent harm to others. [Their] own good, either physical or moral, is not a sufficient warrant. (Wacks 37-38)

In the Liberal tradition, this division is often known as the “public/private split”: in *private* you are free to do anything you want as long as it doesn’t impact anyone else, but in *public* we have responsibilities to the common good—what our UU 6th Principle calls "The goal of world community with peace, liberty, and justice for all.”

Today, however, modern technology has advanced to the point where having any genuine privacy is increasingly elusive. Companies like Google, Apple, Amazon, and Facebook are collecting vast amounts of data about us, often in even our most intimate spaces. So for our modern age, Dr. Westin offers us this working definition of privacy: **“the claim of individuals, groups, or institutions to determine *for themselves* when, how, and to what extent information about them is communicated to others”** (42).

Westin, however, is no longer with us. He died about five years ago. My favorite contemporary guide to the intersection of technology and privacy is Bruce Schneier (1963-). Schneier is an internationally renowned security technologist, who among his many appointment is a fellow at the Harvard University’s Center for Internet & Society. The best introduction I have found to his perspective is his 2015 book Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, but I also recommend his latest book, published just this year, titled Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, which is about the promise and the peril of having an increasing number of things connected to the Internet—meaning that they are also vulnerable to being hacked.

Part of what I appreciate about Schneier is that he is neither anti-technology nor anti-surveillance, but he urges us to be more informed about the potentially dangerous implications of both (Schneier 2015: 10). Consider, for instance, how much data is being collected on us continuously. **With smartphones, “The GPS receiver can pinpoint you to within 16 to 27 feet**; cell towers to about 2,000 feet” (16). With a high degree of accuracy, “Our cell phones reveal where we are at all times, where we work, who we spend time with. They know when we wake up and when we go to sleep…. And because everyone has a cell phone, they know who we sleep with” (Schneier 2018: 58).

The rabbit hole, however, goes much deeper:

- “Purchase something in a store and you produce more data.”

- “There may be a video camera in the store…. There are more cameras outside, monitoring buildings, sidewalks, roadways, and other public spaces.”
- “Get into a car, and you generate yet more data. Modern cars are loaded with computers, producing data on your speed, how hard you’re pressing the pedals, what position the steering wheel is in, and more. Much of that is automatically recorded in a black box recorder, useful for figuring out what happened in an accident.”

Not long ago, someone would have to pay a private investigator a small fortune to collect even a partial slice of this information, but now an increasing number of consumer products have built-in ways to collect this data about us, and to communicate it to corporations and other entities (Schneier 2015: 16-17).

And the rabbit hole goes at least one more level deeper. Corporations are by all means interested in your specific personal data to target you more accurately—or we could say more *creepily*—with advertising (2-3). But they are also interested in the trends that are shown when *everyone’s* data is collected and compared on a mass scale—what is sometimes called “metadata” (6).

On one hand, important changes can come from studying big data to learn about what we humans really do and think—and to equip us with what we really need to improve our quality of life. On the other hand, that same level of access to our personal data can and has been used by corrupt corporations and authoritarian governments for manipulation, intimidation, and social control (2).

Consider the vast amounts of data Google has collected about us—from what has been googled over the years, to what has been typed into Gmail, Google maps, and all the other Google products. As Google’s CEO Eric Schmidt said in 2010, **“We know where you are. We know where you’ve been. We can more or less know what you’re thinking about”** (26).

We can take that confession from our Google Overlords (who mostly want to exploit us for profit) and turn it up to eleven when we consider that “In 2014, former NSA and CIA director Michael Hayden remarked, 'We kill people based on metadata’” (27). Suffice it to say that it does really matter who has access to our data, and what they are empowered to do with it.

And defending our right to "determine *for ourselves* when, how, and to what extent information about us is communicated to others" is also a significant part of our own Unitarian Universalist history. And although there are quite a few different stories we could consider from UU history, one of the most recent is that, "In 2013, the First Unitarian Church of Los Angeles sued the NSA over its domestic spying, claiming that its surveillance of the church members' telephone calling habits discouraged them from banding together to advocate for political causes in violation of the First Amendment freedoms of speech and assembly as well as Fourth Amendment protections against unreasonable search and seizure (107). Let me tell you just a little of the background of how that lawsuit came to be.

In the 1950s and 1960s (starting during McCarthyism), First Unitarian Los Angeles was under FBI surveillance because its longtime minister, The Rev. Stephen Fritchman, was suspected of being a Communist (Eaton 2). Also around this time, this congregation was also on the government's radar because "In 1952, California passed a constitutional amendment requiring religious organizations to sign a loyalty oath in order to keep their tax-exempt status. Along with several other churches, First Unitarian Church refused. It lost its tax-exempt status until 1958, when the Supreme Court ruled the loyalty oath unconstitutional in *First Unitarian Church v. Los Angeles*. (12).

When UU World and others have researched this time period, "An initial Freedom of Information Act request for the FBI's records on First Unitarian of Los Angeles turned up over 5,000 pages…. Fitchman or the church come up in FBI documents that also mention the Rev. Ralph Abernathy, Albert Einstein, Eleanor Roosevelt, and the American Friends Service Committee, to name just a few. Other people who were the subject of FBI files and who probably also raised suspicion—including W.E.B. Du Bois, Langston Hughes, Margaret Mead, Linus Pauling, and Pete Seeger—had spoken at First Unitarian Church" (Eaton 11).

Importantly, this case of the FBI surveillance of First Unitarian L.A. was not isolated. As detailed in other documents acquired through the Freedom of Information Act:

- A 1969 FBI document “discussed open meetings held at First Unitarian Church of South Bend, Indiana by the Michigan Committee to End the War in Vietnam, which a Bureau source claimed was a Communist Party front.”
- Another FBI document from 1969 “described plans by civil rights leader the Rev. Andrew Young to speak at a dinner at Cedar Lane Unitarian Church in Bethesda, Maryland, in memory of the Rev. Dr. Martin Luther King, Jr. The memo noted that the FBI had alerted the Metropolitan Police Department, the Secret Service, and ‘interested military agencies’” (6-7).

As the saying goes, “It’s not paranoid if they really are after you!”

Now, to be clear, my goal is by no means to demonize the FBI, the NSA, or other government agencies when they are acting in good faith to keep us safe. But security must be balanced against privacy and government overreach.

And this historical background is important for understanding why—when the Electronic Frontier Foundation was considering a lawsuit against the National Security Agency “on behalf of a coalition of nonprofits and advocacy organizations over the agency’s mass collection of Americans’ telephone data”—First Unitarian Los Angeles came to mind as a strong potential plaintiff. And so *First Unitarian Church v. NSA* was born (Eaton 2). The latest update I have found is that the case is seemingly stalled permanently at the District Court level due to a number of factors including the passage of new laws by Congress in the government’s favor.

I should also be sure to add that when discussing this topic, the biggest canard that always comes up is that, “You don’t have anything to worry about unless you have something to hide” (Schneier 2015: 147). That cynical claim is misleading for a few different reasons:

1. If you have enough data about someone, you can always find some plausible pretext to embarrass, frighten, misrepresent, discourage, threaten, harass, accuse and/or condemn them. As Cardinal Richelieu said in the seventeenth century, “Show me six lines written by the most honest man in the world, and I will find enough therein to hang him” (108).
2. Even more fundamentally, having times and places where we can truly be private and unobserved is a human right necessary for maintaining our dignity (272).

But in light of twenty-first century technology, protecting any sort of genuinely private space is increasingly difficult. We need more robust laws about our personal ownership rights to data produced by and about ourselves, including some form of the "right to delete," which is sometimes called the "right to be forgotten." Now I don't expect we'll ever see a required reminder before posting on social media that warns, "What you've written will be saved by Facebook and used for marketing, and will be given to the government on demand" (240). But we might obtain more power to tell certain companies in certain instances, **"I'm leaving. Delete all the data you have on me"**—or, "I never gave you permission to gather information about me and sell it to others. I want my data out of your database" (237-238).

For now, in Schneier's assessment, "We're still in the honeymoon phase of connectivity. Governments and corporations are punch-drunk on our data, and the rush to connect everything is driven by an even greater desire for power and market share." But keep your eye out: as we continue to move rapidly toward the surveillance and security end of the spectrum, the demand for freedom and privacy will continue to grow.

From the perspective of our UU Principles:

- Our 1st Principle of each person's inherent *dignity* is violated by invasions of privacy.
- Our 4th Principle of a *free* search for truth and meaning requires privacy from Big Brother watching every move we make.
- And as we have seen, our 5th Principle of the democratic process also requires citizens to have the freedom to organize without the intrusion of government.

Our call is to embrace the freedom that is so central to our individual dignity—and to our collective liberty.