

Our Orwellian Hole

In the internet era, the amount of information we offer up about ourselves is staggering. No one has to dig around for what we freely give. We do it without much thought and seem concerned only when there is a breach revealing our credit card numbers and even then there is a thriving industry to cure that ailment. Practically every app we download to our phones asks us for access to virtually every piece of information we carry around or receive. Then, we appear shocked when our information is used for purposes we did not intend – like unwittingly helping out political campaigns. Now we are excited to spit on a Q-tip and give up our DNA as if every other piece of personal data about ourselves, our relationships and what we buy at the grocery store is not enough. With the advance of artificial intelligence, how long before even a hint of privacy becomes a fantasy. We have no one to blame but ourselves and our addictions to gadgets and social media. After all, it is exciting when Alexa's soothing voice, always peering out at you through her camera and always listening through her microphone, gives you the weather, your appointments and plays your favorite music. The persistent questions are how far have we willingly gone down the Orwellian hole? And can we ever climb out of it? There will always be some willing to take a potential good thing and use it for bad purpose.

Within weeks of the September 11, 2001 terrorist attack, President George W. Bush signed into law the [Patriot Act](#).

There was some debate, but with urgency an overwhelming Congressional majority passed it. There were concerns about electronic surveillance of Americans inside the United States in violation of their rights to freedom of association and freedom of speech. We trusted politicians and political appointees to do the right thing. Following the Ben Franklin axiom, we forfeited some liberty for promised safety.

On the subject, I was one of many fence sitters. I wanted our agencies enabled to collect intelligence and foil terrorist plots. I did not think it likely they would intentionally collect data on average Americans. My naivete also steered me to believe the Government of a free United States of America would never abuse this power to spy on Americans for reasons other than anti-terrorism and especially not political opposition during a Presidential campaign.

Back in 2005, when the political conversations heated up around the subject, I favored the Patriot Act because I chose political sides. If certain people came out against anything rigid thinking automatically compelled to be for it. My thinking has matured some since. Even though I made and received frequent international calls as the NSA was making bulk collection of phone records I expressed concern then that I feared Google more than the remote possibility the National Security Agency would capture my data illegally or otherwise.

Surveilling the landscape today I sort of feel like a prophet – at least as it relates to Google. I also believe that our government intel collection methods capture everything to sort out later if needed. How long before the Russians or Chinese hack them servers?

If you have a Google account, an Android cell phone in your pocket, and use the Chrome web browser you can probably hear the old 80's *The Police* tune *Every Breath You Take* playing in the background.

Every breath you take and every move you make
Every bond you break, every step you take, I'll be watching you
Every single day and every word you say
Every game you play, every night you stay, I'll be watching you

Google not only captures but stores enormous amounts of data

on each of us. Data we offered up freely. The potential for abuse of this data by criminals, unknown intelligence agencies (foreign and domestic), and political parties should concern every American. Especially in light of current events.

Over recent months, we learned unscrupulous people are willing to [abuse the Federal Intelligence Surveillance Act](#) (FISA) to spy on Americans under the guise of monitoring possible foreign agents. It just so happens the foreigners being monitored were having conversations with members of an opposing political party during a Presidential campaign. We've also learned FISA court judges appear, [with a 99.97% approval rate for warrants](#), rubber stamps. Google may actually do a better job protecting our data than the government. With our proven abilities to gather and store vast amounts of data, whose to say [our government doesn't already have its arms wrapped around Google](#) and others. What's the downside? Abuse of this power likely leads to legislation and regulation that hinders our ability to protect ourselves and restricts our ability to freely use the Internet. Or we become Mr. Orwell's totalitarian state. For public consumption, what we write may end up being nailed to a tree.

As our founders reminded, our system of government is designed for law abiding people. With no exceptions, people proven to have illegally abused FISA and illegally spied on Americans must be prosecuted to the fullest extent of the law. The saddest fact? Most people consume only legacy news media and nowadays social media so are literally blind to this abuse.

And then there's Facebook. Facebook also collects data offered up freely by people who decide the need for a Facebook presence – myself among them. It seems we want to be noticed so we readily give up many details about our lives and readily “friend” people we know nothing about giving them access to our personal information. It is something most of us would never do in a face to face conversation with a stranger.

By what you read, what you share, what you like, what products you search for, who you follow, who follows you Facebook can make a relatively accurate assessment of you and your social network. Facebook analyzes and uses this information for lucrative targeted advertising. When you are the world's largest social media network, it's an absolute gold mine.

In terms I can understand, a social graph is a chart that shows relationships between all the people in a community. In the internet era, it's sort of like the universe. It's massive and endless.

As of 2010, **Facebook's social graph** is the largest **social** network dataset in the world, and it contains the largest number of defined relationships between the largest number of people among all websites because it is the most widely used **social** networking service in the world. – [Wikipedia](#)

Facebook has some problems however. They've decided to protect us by deciding what we should post and what we should read. It's that algorithm thing we keep hearing about – the process that decides what's hate speech, what's unsafe, what's fake, and what's real. They want to know all about us and then guide us toward their idea of what's good for us. It is a utopian mindset. It's as if they would prefer to rid the planet of critical thinking. Their other problem is the data they collect with which to target us is also available to or accessible to anyone or organization savvy enough to mine it. They played fast and loose with our data until a company that did not share their worldview used some of it.

Cambridge Analytica is a data analytics company that mines and uses data about what we like, what we share, who we friend, etc. to target political advertising. Their problem, it seems, is they provided data to some conservative campaigns and supposedly to the Trump campaign. These assertions alone led to Congressional hearings. It was unacceptable that a company helping conservative campaigns may have used

information readily available to anyone including President Obama's campaigns. It was so offensive that [Facebook banned](#) them.

Congresswoman Maxine "Impeach Trump" Waters let the cat out of the bag some time ago, but it never broke through the liberal media firewall other than to compliment the genius of Obama's social data mining.

"The president [Obama] has put in place an organization that contains the kind of database that no one has ever seen before in life. That's going to be very, very powerful. That database will have information about everything on every individual in ways that it's never been done before." [Maxine Waters](#)

While Facebook and assorted liberals are throwing a conniption fit about the activity of Cambridge Analytics, they are ignoring the fact that they either provided or allowed access to data on millions of users to [Obama's reelection campaign](#). This could be a violation of federal election law, but don't hold your breath for the investigation to begin.

Carol Davidsen was the Director, Integration and Media Analytics for Obama for America.

"In 2011, Carol Davidsen, director of data integration... and media analytics for Obama for America, built a database of every American voter using the same Facebook developer tool used by Cambridge, known as the social graph API. Any time people used Facebook's log-in button to sign on to the campaign's website, the Obama data scientists were able to access their profile as well as their friends' information. That allowed them to chart the closeness of people's relationships and make estimates about which people would be most likely to influence other people in their network to vote.

"We ingested the entire U.S. social graph," Davidsen said in an interview. "We would ask permission to basically scrape

your profile, and also scrape your friends, basically anything that was available to scrape. We scraped it all.” – [The Washington Post](#)

“We ingested the entire U.S. social graph.” In other words, millions of “friends” had their data sucked up without their knowledge or consent. According to Davidsen, Facebook was really broken up by this revelation. She recently Tweeted:

“They came to office in the days following election recruiting & were very candid that they allowed us to do things they wouldn’t have allowed someone else to do because they were on our side,” – Carol Davidsen – [The Daily Caller](#)

Whether it is information swept up by NSA surveillance or what we freely give to Facebook, Google, Twitter, LinkedIn, et al we have made ourselves vulnerable to manipulation and misinformation campaigns. We have allowed others, using psychological graphs and other tools, to guide us. They want to guide our thinking, steer us toward the news and information some “algorithm” has determined is safe for us. Being human, we like the easy route so we are likely to go where the search engine leads. We prefer to follow rather than lead and our youth are the most susceptible. It’s brainwashing on a sophisticated global scale. Survival requires us to start searching for the way out of the Orwellian hole we’ve dug for ourselves.

© 2018 JD Pendry – All Rights Reserved

E-Mail JD Pendry: jd@jdpendry.com