افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــــاد بدین بوم وبر زنده یک تن مــــباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com afgazad@gmail.com

European Languages	زبان های اروپائی

http://www.counterpunch.org/2013/10/29/the-corporate-state-of-surveillance/

The Corporate State of Surveillance

by RALPH NADER

October 29, 2013

America was founded on the ideals of personal liberty, freedom and democracy. Unfortunately, mass spying, surveillance and the unending collection of personal data threaten to undermine civil liberties and our privacy rights. What started as a necessary means of reconnaissance and intelligence gathering during World War II has escalated into an out-of-control snoop state where entities both governmental and commercial are desperate for as much data as they can grab. We find ourselves in the midst of an all-out invasion on what's-none-of-their-business and its coming from both government and corporate sources. Snooping and data collection have become big business. Nothing is out of their bounds anymore.

The Patriot Act-enabled National Security Agency (NSA) certainly blazed one trail. The disclosures provided by Edward Snowden has brought into light the worst fears that critics of the overwrought Patriot Act expressed back in 2001. The national security state has given a blank check to the paranoid intelligence community to gather data on nearly everyone. Internet and telephone communications of millions of American citizens and millions more citizens and leaders of other countries. Even friendly ones such as Germany, France and Brazil have been surveillance targets –over 30 foreign leaders such as German Chancellor Angela Merkel and Brazilian president Dilma Rousseff have reportedly been targeted by this dragnet style data-collecting. More blatantly, covert devices were reportedly placed in European Union offices and earlier by Hillary Clinton's State Department on the United Nations to eavesdrop on diplomats. World leaders are not pleased, to put it mildly.

Many Americans are not pleased either. And while most of the recent public outrage in the U.S. has been directed at instances of government snooping, giant private corporations are equally as guilty of the troubling invasion of peoples' selves. Companies such as Google, Apple, Microsoft and Facebook blatantly collect and commercialize personal data — often covering their tracks with complicated fine-print user agreement contracts that most people, whose property it is, "agree" to without any consideration. Clicking "I agree" on an expansive, non-negotiable user agreement for a website or a software program is, to most people, just another mindless click of the mouse in the signup process.

These "take-it-or-leave-it" contracts leave the consumer with little power to protect their own interest. (See here for our extensive work on this issue. Also, visit "Terms of Service; Didn't Read" for a valuable resource that summarizes and reviews online contracts so that users can have a better understanding of what they are agreeing to.)

Just last week, news broke that Google plans to roll out a new advertising feature called "Shared Endorsements." This policy allows Google the right to create user endorsements in online advertisements. So, if a Googler happens to share their preference for a particular product online, his or her endorsement might end up featured in an ad without any notice or compensation. Of course, users are welcome to "opt-out" of this program — but how many millions will remain ignorant of the fact that they unwillingly opted-in by clicking their consent to contract terms they did not bother to read out of habit. (Google's official statement claims the move is to "ensure that your recommendations reach the people you care about.")

Opting-out should be the default option for all these types of agreements.

School children are also being targeted by mass data collectors. InBloom, a nonprofit organization based in Atlanta, offers a database solution for student records between grades K-12. In theory, this service is supposed to make it easier for teachers to utilize emerging educational products and tools. But in practice, many parents are concerned about how this data will be used — in one instance, for example, student social security numbers were uploaded to the service. One parent told the *New York Times*:

It's a new experiment in centralizing massive metadata on children to share with vendors… and then the vendors will profit by marketing their learning products, their apps, their curriculum materials, their video games, back to our kids.

Facebook poses another data mining risk for young children. Although Facebook does not currently allow children younger than 13 to join — the Children's Online Privacy Protection Act prevents the online collection of data of children without parental permission — reportedly more than five million underage children use the social media website anyway. This exposes them (and their personal information) to thousands of advertisers that use Facebook to collect marketing data and promote their products. See the Center for Digital Democracy's recent report "Five Reasons Why Facebook is Not Suitable For Children Under 13." Notably, Facebook recently changed their privacy policy to allow teenagers between the ages of 13 and 17 to opt-in to sharing their postings with the entire world, as opposed to just their "friend network."

The insatiable appetite for data is reaching beyond the digital realm, as well.

The *Washington Post* recently reported that Mondelez International, the company behind snack brands like Chips Ahoy and Ritz, has plans to deploy electronic camera sensors in snack food shelves to collect shopper data. These "smart shelves" can scan and save a customer's facial structure, age, weight and even detect if they picked something up off the shelf. The device can then use that gathered data to target the consumers with "personalized ads." For example, at the checkout line, a video screen might offer you 10 percent off the box of cookies you picked up but ultimately chose not to purchase. The *Post*reports: "The company expects the shelf to help funnel more of the right products to the right consumers, and even convince undecideds to commit to an impulse buy."

The smart shelf builds on the Microsoft "Kinect" camera technology, which has the ability to scan and remember faces, detect movement and even read heart beats. Microsoft developed the Kinect camera as a video game control device for the home. In light of Microsoft's reported connection to the NSA PRISM data gathering program, why would anyone willingly bring such a sophisticated spy cam into their living room?

Along the same lines, certain retailers are using smart phones to track the movement of customers in their store to gather information on what products they look at and for how long — similar to how Amazon tracks online shopper habits so it can direct them to other products that algorithms determine they might be interested in. Sen. Chuck Schumer (D-NY) has called on the Federal Trade Commission to regulate this disturbing practice. He recently announced a deal with eight analytic companies to institute a "code of conduct" for utilizing this seemingly Orwellian technology. Sen. Schumer told the *Associated Press*: "When you go into your store for your Christmas shopping, there'll be a sign out there that says that you're being tracked and if you don't want to be, you can very simply opt out." The details on how exactly one opts-out of this invasive technology, short of leaving their cell phone at home, is not yet clear.

With all these instances of Big Brother encroachment, one might want to opt out of the digital world entirely, and avoid supermarkets and retail chains that spy on customers. Unfortunately, that is becoming more and more difficult in an increasingly technology-obsessed world.

It's time for citizens to stand up and demand their right to privacy, which is a personal property. Mass surveillance and rampant data collection are not acceptable and should not be the status quo. Recall that there was once a time when the federal government could defend our nation without limitless access to computer records, emails, online search histories and wiretapping phone calls without open judicial authorization. Businesses could be successful without tracking and saving your shopping habits and student records were not commodities to be traded away. Why do they now do what they do? Because they can.

Remember, what you allow to be taken from you by the private companies can also end up in the files of government agencies.

This Saturday, a coalition of groups including the ACLU, Public Citizen, the Electronic Privacy Information Center (EPIC), the Libertarian Party and many more are gathering on the National

Mall to protest mass surveillance by the National Security Agency. This is a positive first step in letting our elected officials know that ceasing the collection of private personal information about you is important and mass surveillance should be prohibited. Visit here for more information about this weekend's rally. Join the movement to end these burgeoning, tyranny-building abuses by runaway federal agencies.