FOREIGN POLICY RESEARCH INSTITUTE
E-NOTES
June 2013

PRIVACY REFRACTED THROUGH PRISM

By Lawrence Husick

Lawrence Husick is an FPRI Senior Fellow, Co-Chair of FPRI's Center for the Study of Terrorism, and Co-director of FPRI's Wachman Center project on Teaching about Innovation.

Twenty years ago, at the dawn of the Internet age, I demonstrated the nascent power of database research to inform, embarrass, and anger a legal colleague. In full public view during a legal education seminar about the Internet, and without spending a cent, knowing only the name and law firm affiliation of a random member of the seminar audience, I constructed a personal dossier. Gathering then-available records using public sources and simple database queries, I proceeded from name to address, to taxes paid, debts owed, family names, schools, locations, and ages, marital status and assets. Moving on, and without breaking any laws, I determined credit histories, court cases and judgments, employment history, volunteer involvements, political leanings, contributions, and other information about my unwilling subject so personal that in a matter of minutes, I was heatedly accused of what amounted to digital witchcraft, echoing Arthur C. Clarke's Third Law that, "any sufficiently advanced technology is indistinguishable from magic."

In the time since, the lives of most citizens in the developed world have become even more cataloged. We move through a digital sea, leaving in our wake vast amounts of disjointed data and ripples that spread outward, waiting to be interpreted in ways that we cannot imagine. We live in this world, tucked into an illusion of privacy that vanished long ago without a trace or a whimper, and despite numerous "wake up calls" from the American Civil Liberties Union, the Electronic Privacy Information Center, and the Electronic Frontier Foundation, we continue to hope that our privacy will be protected and our anonymity will be secured, if only by our own personal obscurity. (The "why would they be interested in little-old me?" school of thought.)

In the wake of recent revelations about the National Security Agency's PRISM and Boundless Informant efforts, we are again confronted with the reality that our sense of privacy is illusory. The questions facing Americans and others must now include issues of the proper roles of government and corporations in collecting and analyzing our personal information, and the degree to which such activities are to be limited by law, given our inability to "opt out" or to live "off the grid" in our daily lives. As Benjamin Franklin wrote in Poor Richard's Almanac in 1755, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." What, then, is our "essential" liberty, and how permanent is the safety promised by massive governmental (and corporate) data collection and mining?

To understand the scope of the problem, an analogy to a popular genre of television program may be useful. In the "CSI" programs, we have come to understand that each of us sheds millions of microscopic particles as we live our lives. Flakes of dead skin, strands of hair, saliva on envelopes and from sneezes, tracked pollen, dirt, bacteria…the detritus of just being, all waits to be collected, sorted, and analyzed by skilled forensic technician heroes who catch the bad guys before they strike again. So, too, our digital detritus tells our stories in unseen and unsuspected ways. Each credit transaction, text message, telephone call, toll booth, parking gate, card swipe, pay-per-view, channel

change, travel reservation, and thousands of other daily digital "dots" is being vacuumed up and stored in warehouses that dwarf the final scene in "Raiders of the Last Ark." According to the grey heads of intelligence, this data is just collected, becoming the "haystack" to be searched retrospectively when an incident requires, and we have no cause for concern. But young analysts like Edward Snowden, a 29 year old high school dropout with a sudden sense of outrage have built software tools of vast power and reach, and seem to have done so at the command of their private sector employers in the service of intelligence agencies. These digital forensic detectives have used the power of government to gain continuous, if not "direct" access to the data representing the lives of billions of people, and have used the power of publicly-available "big data" systems to create software that can accurately represent almost every aspect of a person's life in society.

It has long been known that Chinese intelligence gathering relies on the collection of vast amounts of public information (in addition to covert espionage directed at classified and confidential data.) By correlating and aligning public information, patterns emerge from which private information may be discerned. Last week, amid the leaks about the NSA programs of digital spying, President Obama addressed this issue with Chinese President Xi Jinping. (Such open-source sleuthing was the concern of the Department of Defense that delayed the publication of Tom Clancy's novel "The Hunt for Red October," even though Mr. Clancy carefully documented the public source of each fact on which he based the technology described in the book.)

It is now clear that US intelligence agencies have been engaged in massive, digital "quilting bees" – using sophisticated computers to piece and stitch together the fragmentary intricate details of the lives of every citizen engaged in digital commerce, public movement, and telecommunications – in short, every person living a modern life. The spooks may not be, "listening to your telephone calls" as President Obama insisted, but they may not need to.

Many Americans came of age under 1960's laws which tightly regulated wiretapping and "trap and trace" recording of telephone communications by the government by imposing various warrant requirements. The USA PATRIOT (Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism) act changed almost all of those regulations, giving the federal government sweeping automatic powers to collect the kinds of communication information that were previously restricted. Despite four-year sunset provisions, the law has been renewed each time it has been set to expire, and in some instances, broadened in scope. The government now routinely uses National Security Letters to obtain billions of pieces of digital information which it stores and processes. Under the law, the companies receiving those directives cannot reveal them, or even challenge them in court. According to the text of top secret Presidential Policy Directive 20, released by the hacktivist group "Anonymous", the United States may also conduct "Cyber Collection" activities, even if doing so would manipulate, disrupt, degrade or destroy computers, systems, networks, or infrastructure.

How, then, should citizens and their elected and appointed officials evaluate now-declassified programs such as PRISM, and the many still-classified others of unknown scope and effect? Are the locations of our mobile telephones and computers, the contents of our text messages and emails, and our digitally-recorded comings and goings all an open book? Or, as Justice Bradley, and later, Justice Douglas put it, are the Fourth and Fifth Amendments, "protection against all governmental invasions 'of the sanctity of a man's home and the privacies of life.'" Should privacy be viewed, as that angry attorney twenty years ago asserted, in light of the power to assemble and interpret information conferred by computers, databases and networks? Is that privacy an "essential" freedom, in Franklin's formulation, or, as the Facebook generation seems to believe, is privacy obsolete? If privacy is essential, then how permanent is the safety being purchased? If our government will not tell us in the name of national security, how can we judge?