Written by **Beverly K. Eakman** on December 8, 2011

Surveillance Technology Takes a New Twist, Morphs Again

It was reported in Tuesday's Washington Times, among other places, that surveillance technology has taken yet another turn, this time bringing military-grade, high-tech surveillance tools originally intended for intelligence-gathering to the marketplace, enabling even relatively unsophisticated users to snoop on friends, neighbors, significant-others — and political opponents.

As if massive prying by government agencies to track and monitor everything from an individual's whereabouts to keystrokes were not enough; as if spammers' and advertisers' capability to place spyware and "cookies" on everybody's personal computers were not part and parcel of today's marketing strategies; as if tapping into e-mails, websites, and phone conversations were insufficient to satisfy the curious; as if collecting and cross-matching information gleaned from intimate questionnaires and surveys in the name of "education" had not all but superseded academics, now comes news that cybersurveillance has gone global — and that America is partnering with some of the worst foreign offenders.

One German company, states the *Times* report, sells a British-designed cyber-package called FinFisher, bringing new meaning to the term "private-public partnership." FinFisher boasts the capability to "identify an individual's location, their associates and members of a group, such as political opponents." Such capabilities, of course, have been available for some time — but *separately*, not in one package, and not for average consumers. Now all that is necessary for any entity, from disgruntled opportunists to activist organizations or a cartel, to buy a piece of the action is spare cash. And with enough fingers in the same cyber-surveillance pie comes the potential of conflicting influences — not to mention windfall profits — quite enough to serve as a tool of blackmail.

Washington Times reporter Shaun Waterman, in his front-page story, divulged that technologies which were once "the exclusive preserve of … government spy bureaus … are now available to the highest bidders from companies in dozens of countries." The latest gee-whiz cyber-tools are essentially unregulated and, in the wrong hands, threaten to become game-changers in a brave new psycho-political world which partners adversaries with supposed allies. Never mind that "[o]ne or more fast-growing regional powers may judge that changes in its economic and political interests merit the risk of aggressive cyber and other espionage against U.S. technologies and economic information."

For example, Russia's biometric voice-recognition technology has moved beyond what most of us understand as individual voice-pattern fragments compared against a database of other voices to come up with what is hopefully a unique identifier, now it can "isolate and identify hundreds of individually targeted voices from daily digital recordings of thousands of phone calls." This means singling out voices from among groups *all talking at once*. Waterman points out that all high-tech cyber-companies say they operate within the law, selling only to government, especially law-enforcement, "and other authorized users" — not exactly a warm-and-fuzzy prospect in itself, given the overkill with which America's own Transportation Security Administration has carried out its anti-terrorism task. The new cyber-technologies enable anything selling itself as "law enforcement" to become its own self-contained little fiefdom — a mini-KGB or a Stasi.

As for "other authorized users," just who, or what, might be authorizing them? The local drug cartel? Sales mean money, after all, and one need look no further than the recent "Fast and Furious" scandal, or the infamous and violent Mexican Zeta/MS-13 gangs — both of which have exported themselves and moved their operations into America — to know that even the most sophisticated technologies have already fallen into the hands of criminal organizations. Global terrorist networks such as al Qaeda, Hamas, and Hezbollah, as well as organized crime operations such as the Russian Mafia now conceivably can have tentacles anywhere they want to insert themselves, including into American politics.

China hypes "software that can crack the security" on various popular Internet e-mail accounts. Other firms offer packages that have the capability to "eavesdrop on cell phone calls, … tap into fiberoptic cable …, [and even] search, filter and index" vast quantities of data to obtain what buyers need or want, according to Waterman's research.

And therein lies the twist — not specifically alluded to in either Waterman's report or any other analysis of the subject. Just as film editors can keep those parts of footage that producers like, and consign those portions that don't pass muster to the cutting-room floor, so can end-users of these once-secret technologies, so beloved of spy bureaus like the National Security Agency and its counterparts in hostile countries, apply the same "creativity" to political opponents and candidates in government. They can use the technologies to marginalize candidates in the media, neutralize opponents or advocates before they ever reach busy legislators, ridicule and malign even articulate professionals with the public. *By the time the time the victim gets around to launching a libel suit, the damage is done:* Events move on and any "evidence" (such as it is) is corrupted so as not to be viable in a court of law.

To simplify: Suppose a sharp candidate for some lower-level public office such as school board advocates a position diametrically opposed to the status quo. Computer hackers uncover a prescription tranquilizer for diazepam. Privacy laws involving doctor-patient confidentiality and pharmacy pickups notwithstanding, political opponents are made aware of all the candidate's medications, "diazepam" having been picked out from among those prescribed. Armed with the delivery or signature dates, Rx numbers, and phone numbers cross-referenced for identification purposes, the candidate's opponents proceed to publicize "diazepam," intimating (but not saying outright) that the candidate is mentally unstable. The missing information — the piece of data now lying on the equivalent of the "cutting room floor" — is lockjaw. The patient had a procedure or condition that resulted in lockjaw. Diazepam is among the least invasive treatments shown to alleviate the situation. The drug is usually effective if taken for even a short time. Ironically, doctor-patient confidentiality and pharmacy privacy laws will serve not to help the candidate, but rather to keep a lid on the real reason for treatment. Unless it is the

President of the United States or Speaker of the House under scrutiny, any privacy waiver involving public disclosure will come much too late to save our intrepid candidate.

Individuals who might otherwise run for public office already fear the media, greatly diminishing the pool of contenders. What folks typically don't know is the means by which information is "sliced and diced" for public consumption by political enemies — then surreptitiously fed to the media. By the time the aspiring office-seeker finds out who hacked information, who leaked it to the press, and how any actual positions on the issues got lost in the shuffle, the contender has become the butt of late-night jokes. As with the candidate who was prescribed diazepam, a "mental instability" innuendo will follow indefinitely. Libel suits for someone *already* in the public eye come under the rubric of a "public figure" — still extremely difficult and expensive to prove, and "malice" even more so. But a candidate who comes out of nowhere can expect to be hounded unmercifully without the backing of what has become America's ruling caste.

Now, even that may not be enough for foreign activists — entities with enough money to buy influence over U.S. policies. According to the Office of the Director of National Intelligence's *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, which includes a section on political espionage, "cyberspace provides [even] relatively small-scale actors an opportunity to become players in economic espionage.... Similarly, political or social activists may use the tools of economic espionage against U.S. companies, agencies, or other entities, with disgruntled insiders leaking information about corporate trade secrets or critical U.S. technology to "hacktivist" groups like WikiLeaks."

When Americans go to movies and stare wide-eyed at the special effects, they come away so mesmerized by ultra-sophisticated technologies they may forget that there was barely any plot. Similarly, when they go to the polls, they do so in the shadow of technologies which were once tightly kept secrets of spy-masters. We live in an era when it is possible to put one person's head on another's body — and make it convincing to all but the forensic computer specialist. It is no stretch to say that technology has outpaced the legal system — not only our own, but *every* legal system. And that was *before* the wares of foreign intelligence services were being sold and purchased so Americans can cyber-bully each other!

"Sure it's illegal...," says privacy advocate Christopher Soghian, a fellow at CACR, the Center for Applied Cybersecurity Research, Indiana University, as quoted in the *Times* piece, "...but you're never going to get caught." That is to say, all the ethical guidelines and precautions that should have been put in place back in the early 1990s didn't happen. As technology is never "un-invented," but rather is only superseded by a better version, we are all now actors in a self-made sci-fi flick where the machines outmaneuver their masters. As Emily Draper, spokeswoman for an outfit called Privacy International, put to Waterman for his *Times* article: "The fact [is] that [foreign] companies are selling what are essentially tools of political control to oppressive regimes with impunity...."

How many companies? Some 130 worldwide, according to CACR's Christopher Soghian. Even the fairly computer-literate are hard-pressed to keep up with what's "out there": India's Paladion, Israel's Covertix, and many more in Germany, Brazil, and Russia. Our nation's leaders are playing with fire by encouraging inroads into U.S. markets.

Ironically, national security officials say the United States, even with all its shock-and-awe gizmos, has nothing that tops what many foreign countries, and even terror-sponsoring groups, are selling — though certainly not for lack of trying. American purveyors of infiltration, interception, and encryption software

are scrambling to compete, not sound the alarm over privacy concerns.

The consequences would flummox today's dying Pearl Harbor generation. Take, for example, the aforementioned FinFisher. It makes Americans even forget they *have* such a thing as Fourth Amendment rights. According to Rep. Robert Hurt (R-Va.), appointed to the Cybersecurity Task Force under the Committee on Financial Services, FinFisher "provide[s] an array of tools and training to let government agents capture everything from your phone and computer, and even control it remotely without your knowing … making it seem that *you* [are controlling] it."

This brings new meaning to manipulation. Learning to recognize lead-in phrases and buzz-terms in order to avoid being manipulated by provocateurs-*cum*-facilitators in meetings and on task forces is almost small potatoes compared to battling technologies that individuals believe they are steering, but aren't!

Meanwhile, television and movies continue to normalize surveillance technologies — usually in the context of crime-fighting, traffic-safety and thwarting terrorism. But when average citizens pull that lever or press that electronic touch-screen to cast their vote, they may wonder: Why is the candidate we were told "had no chance" — despite astronomical amounts of monies raised, straw polls won and debates "aced" — inexplicably absent from the ballot?

_____

B*everly K. Eakman began her career as a teacher in 1968. She left to become a science writer for a NASA contractor, then editor-in-chief of NASA's newspaper in Houston. She later served as a speechwriter and research-writer for the director of Voice of America under the U.S. Information Agency, and two other federal entities, including the U.S. Dept. of Justice. She has since penned six books, scores of feature articles and op-eds covering education policy, mental-health, data-trafficking, science, privacy and political strategy. Her e-mail, a detailed bio, speaking appearances and links to her books can all be found on her website:* www.BeverlyE.com.

Related article: WikiLeaks Exposing "Mass Surveillance Industry"