Published on *The National Law Review* https://natlawreview.com

News Scan Finds Multiple Threats to Your Privacy

Article By:

Theodore F. Claypoole

Your personal information is threatened by more pernicious tools and attacks each year.

While this blog often describes poorly written privacy laws stifling business and dangerous bureaucratic overreach by privacy regulators, it will not lose sight of the metastasizing threats posed to our information. We need to be aware of these hazards and protect ourselves.

A recent scan of privacy articles from the past month surfaced a surprisingly intrusive and varied set of threats to our personal and lifestyle information. The most troubling is the explosion of readily available stalkerware programs that all people could use to surreptitiously track the people in their lives.

A recent New York Times article discussed stalkerware, stating, “While these apps numbered in the hundreds a few years ago, they have since grown into the thousands. They are widely available on Google’s Play Store and to a lesser degree on Apple’s App Store, often with innocuous names like MobileTool, Agent and Cerberus. And they have become such a tool for digital domestic abuse that Apple and Google have started in the last year acknowledging that the apps are an issue. From last September to May, the number of devices infected with stalkerware jumped 63 percent.” The FTC recently instituted its first ban of a stalkerware product, SpyFone from Support King.

Spyware is not without valid and moral applications. Many families use these tools to monitor the safety of young children when away from home, caretakers of elderly people with memory problems apply tracking tools to reduce vulnerabilities, and even adult partners and friends consent to being monitored in certain ways by people close to them. It is use of these spyware products without the consent of the data subject that turns the tools into stalkerware. For example, some of the spyware products hide under an icon for calculator or calendar apps. Much anti-virus software does not search for these products, so finding stalkerware surreptitiously placed on your phone can be difficult.

Cyberstalking is closely tied to sexual violence against women. According to a Kaspersky study, with the help of stalkerware, an abusive person stalking another can [quoted]

- Read anything the surveilled person types – logging each keystroke on the device, including credentials to any kind of services such as banking applications, online shops and social networks, etc.

- Know where they are – by tracking a person's movements with GPS, in real time
- Hear what they say – eavesdrop on calls, or even record them
- Read messages on any messenger, regardless of whether encryption is used
- Monitor social network activity
- See photos and videos
- Switch on the camera

Generally, this information is collected from the mobile device of the surveilled person, and either sent clandestinely to the stalker's computer or saved for a later time when the stalker has access to the victim's phone. The growth of these intrusive tools and ease of use bodes poorly for our personal privacy.

While phone app stalking is getting easier, so is gathering information from personal wearable devices. ZDNet reported last month that over sixty million fitness tracker records were exposed in a completely unsecured database operated by GetHealth. The information exposed included names, birth dates, weight and GPS tracking data. The exposed data was from users all over the world. We know this kind of data can be used not only for stalking individuals, but for choosing targets for robbery or fraud (and understanding their daily patterns), and for identifying the classified locations of military personnel. ZDNet did not share whether heart rates or other health matters usually monitored by wearable fitness trackers were included in this cache of exposed data.

Another of the most troubling privacy threats of the month involves law enforcement. The Wall Street Journal reported that US police and federal law enforcement are using private data services to quietly secure information that would otherwise require warrants to attain, thus bypassing judicial process in place to protect U.S. citizens' Constitutional rights. Law enforcement calls this resource "open-source intelligence" rather than unconstitutional warrantless surveillance. Either description would be accurate. The Journal notes that police omit this mode of surveillance from the records of people arrested after use of this data.

The Journal reports, "Data brokers sprung up to help marketers and advertisers better communicate with consumers. But over the past few decades, they have created products that cater to the law-enforcement, homeland-security and national-security markets. Their troves of data on consumer addresses, purchases, and online and offline behavior have increasingly been used to screen airline passengers, find and track criminal suspects, and enforce immigration and counterterrorism laws." So the sources of data have proliferated so broadly that multiple channels of surveillance are available to those who chose to use it.

Senators Ron Wyden of Oregon and Rand Paul of Kentucky have proposed a bill called "The Fourth Amendment Is Not For Sale Act" which seeks to reduce warrantless police searches by requiring a court order before purchasing cell phone location data from data brokers. The bill would still allow private "volunteers" to buy or gather such data and provide it to law enforcement.

Another frightening infringement of privacy reported by the Journal (they were on a dystopic roll last month) involved school districts using artificial intelligence software to analyze the emotional states of

students. The article says that this software “can scan student communications and web searches on school-issued devices—and even devices that are logged in via school networks—for signs of suicidal ideation, violence against fellow students, bullying and more. Included in the scans are emails and chats between friends, as well as student musings composed in Google Docs or Microsoft Word. When the AI recognizes certain key phrases, these systems typically send an alert to school administrators and counselors, who then determine whether an intervention with the student and parents is warranted.” Schools use the software to look for dangerous behavior and planning, but it can be used to identify anxiety, depression and eating disorders among students.

Of course, these uses sound positive, and applied in the right manner, the tool can be important. But keep in mind the Lower Marion School District of Pennsylvania that loaned laptops to its students who needed them for classwork, but the local IT guys turned on the laptop cameras to watch into the students’ bedrooms. It is one thing to expect minimal abuse from federally trained professionals, and another to hold out such hopes for the underpaid staff of resource-starved public schools. Also, we all know that schools are tight-knit communities where information – even secret information – can flow like water. In a recent survey 81% of teachers said their school uses some form of student monitoring software.

I had identified two other stories from last month demonstrating surveillance that we would not have expected, but after the above discussion I am too depressed to write more. I’m sure some AI somewhere will take note of this fact.

National Law Review, Volume XI, Number 278