InsideCounsel.com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
November 26, 2014

PRIVACY

Preparing for Biometrics and Drones in the 'Post-Privacy' Era

BY HON. CANDACE COOPER (RET.)

Privacy is generally understood as a freedom from unauthorized intrusions. The development of the legal protection of our privacy rights was historically tied to traditional concepts of home, curtilage or property. As frequently articulated, our privacy rights were connected to a "thing" or a "place" where we had a reasonable expectation of privacy. This concept transitioned over time from a physical place to include information space. Now the astonishing developments resulting from modern technologies is further challenging our historic conceptions of privacy and will require the formulation of new standards and practices and perhaps even a redefinition of privacy itself.

Gone are the days when the government only kept records of events such as birth, marriage, property ownership or death. Governments are now using surveillance technologies from drones to automated license plate readers to collect and store data on citizens and non-citizens alike. The commercial collection of personal data is also widespread. Mall owners use technology to track shoppers by signals from their cell phone. Online advertisers and data brokers watch as you browse the web and collect your browsing history. Retailers use digital signs, which are disguised facial recognition scanners, to track your passage through the store for later marketing use. Technologies, like facial recognition software, are even being made available for personal use. For example, Facebook's tagging feature uses this technology.

One type of data being widely collected is biometric information. Biometrics are unique data markers that identify using intrinsic physical or behavioral characteristics. Physical characteristics can include: fingerprints, face prints (facial recognition-ready photographs), iris scan, palm prints, voice prints, wrist veins, hand geometry, a person's gait, and DNA. Behavioral biometrics include non-biological or non -physiological features such as distinctive and unique mannerisms (signature or keystroke patterns, habitual behaviors.) While fingerprints have been collected for generations, technology now allows the real-time capture of many more forms of biometric information. Advances in digital storage technology enables the permanent storage of massive amounts of extraordinarily detailed data.

Data collection is now easily accomplished and does not necessarily require your cooperation or awareness. Governmental agencies, particularly those involved with public safety, are major collectors of data. The United States government operates some of the largest biometric identification systems in the world. The Department of Homeland Security maintains an automated biometric identification system (IDENT) that has a database of more than 126 million records and conducts about 250,000 biometric transactions per day averaging 10 seconds or less per transaction. The DHS Biometric Optical Surveillance System (BOSS) can perform real-time facial recognition and also capture your iris data from 10 meters away … while you are in motion. It was reported in 2011 that the measured error rate in face recognition has dropped by half every two years.

As biometric technology has expanded, so has the ability to store and communicate such data. Stored data may be shared by local, regional, statewide or federal databases or by private companies under contract with a local law enforcement agency. Most local and national law enforcement agencies are working to make the communication between their various databases seamless and responses to queries rapid and accurate. The ability to integrate and store information from many different databases has dramatically increased the value of biometric data and the risks associated with collecting and maintaining it.

The aggregation of dates from multiple sources can pose a privacy threat. There is the risk of theft of biometric information, which could facilitate criminal access to bank accounts and credit cards, allowing the possibility of other criminal activities. There is a risk of data creep, where information voluntarily provided to one recipient may be transferred without permission to another recipient, then linked with other data or applied to a new and unauthorized purpose. At the same time, the unregulated scope of data collection, sharing, linking and storing could invite misuse.

Another medium for data collection that could have far reaching privacy implications is the use of "unmanned air vehicles" or "drones." Previously used extensively only in military applications, the Federal Aviation Administration predicts there will be 10,000 commercial drones by 2017. The FAA has until September 2015 to create rules about how drones can operate in U.S. airspace, and is currently working with several industries to expedite some limited commercial operations. Google has applied to DOT to test its planned U.S. delivery service Prime Air.

There are many legitimate and exciting uses for commercial drones, like emergency response and recovery efforts; mapping and survey applications; television and motion picture industry uses, such as sporting events (i.e., birds' eye view of football game) or special effect shots; agricultural applications; journalistic uses ["journo-drones"]; and "ambulance" drones.

But in the area of privacy related to searches or surveillance, drones are a part of a technology system that acquires evidence that formerly required a trespass. Drones may be equipped with the following types of technologies: high-resolution digital camera, optically or acoustical enhanced imaging; imaging radar [i.e., see thru smoke, haze and other opaque media] or sensors [data re: weather, temperature, radiation or other environmental information). A "perch-and-stare" drone can conduct long-term covert, warrantless surveillance of a suspect.

The use of drones raises myriad ethical and legal issues and presents a situation where the analysis and resolution of those issues lags far behind the technology. The military usage of drones is already well established and the expansion into the civil society is ready to explode. Private parties and corporations are seeking permission to utilize drones before the FAA has even finished developing the regulations that will control their use. Sophisticated drones have the capacity for machine recognition of faces, behaviors, and the monitoring of individual conversations. The images and data collected by drones raise serious questions regarding privacy, data storage and personal liberty.

Both penal and civil laws need to keep pace with these advances. The FAA is creating the administrative regulations and guidelines that will theoretically control the introduction of drones into civil society. Legislation designed to regulate the use of drones has been introduced in the U.S. Congress and in several states. Federal and state law enforcement agencies will have the dual, and potentially conflicting, desire to utilize drones and simultaneously recognize and protect the privacy rights of citizens.

Privacy advocates have raised the alert and the legal community needs to anticipate and prepare for how to protect against the excesses and abuses that could arise from the widespread use of drones. Although the specifics of the incidents cannot be predicted, it is certain that the surveillance abilities of drones will be utilized for industrial espionage and the theft of corporate secrets. Smart counsel should be preparing to advise their clients how to protect and defend against the "coming of the drones."

Hon. Candace Cooper (Ret.) has nearly 30 years of judicial experience and earned a reputation as a highly accomplished judge with a common sense approach to resolving disputes. Based out of the JAMS Los Angeles location, she brings a wealth of legal expertise in handling complex, often highly publicized cases. She can be reached at ccooper@jamsadr.com.