

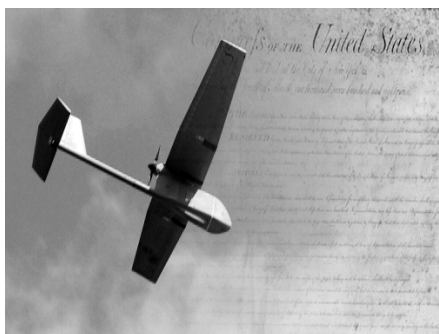
Working to Increase Privacy Protections

A civil liberties briefing



WORKING TO INCREASE PRIVACY PROTECTIONS

Ohioans of all political parties want their personal privacy protected, and to be free from intrusive government surveillance. Privacy concerns identified by the ACLU of Ohio include the **warrantless use of drones and cell phone location tracking; the use of automatic license plate readers by police; and employers and school officials demanding access to employee and student social networking profiles.**



DRONES

Drones are unmanned aerial vehicles which are controlled by a human operator and are used by government and the private sector for a variety of purposes. The Heritage Foundation¹, the International Association of Chiefs of Police², the national Republican Party³, and the ACLU agree that domestic drone use should be well-regulated to protect against unreasonable governmental intrusion through domestic drone use.

The ACLU of Ohio recommends legislation to regulate the use of drones in Ohio. This legislation should require that:

- Warrants are obtained prior to drone use.
- Retention and sharing policies are created for images.
- Explicit, written and public policies and procedures are in place for the use of drones.
- Independent audits of drone deployment are conducted.



AUTOMATED LICENSE PLATE RECOGNITION (ALPR)

ALPR technology is used by law enforcement agencies across the state. It consists of high-speed cameras mounted on vehicles or stationary objects (such as telephone poles or overpasses). The cameras snap pictures of every license plate that passes – capturing thousands of cars' information per minute. A computer checks the information in these pictures against police department databases. If a scanned plate matches information in the database, an officer is alerted. ALPR can be a useful tool for police officers, helping them recover stolen cars and arrest people with outstanding warrants. However, narrow guidelines must be implemented to protect Ohioans' right to privacy.

The ACLU of Ohio would like to see legislation passed in Ohio which:

- Limits the amount of time that captured plate data can be retained;
- Limits the number of authorized uses for ALPR and the number of databases captured plate data can be checked against;
- Prohibits secondary use of data; and
- Requires external audits of the use of ALPR technology by law enforcement agencies.

¹ The Heritage Foundation. [2012]. Drones in U.S. airspace: Principles for governance. Retrieved from <http://report.heritage.org/bg2732>.

² International Association of Chiefs of Police Aviation Committee. [2012]. Recommended guidelines for the use of unmanned aircraft.

Retrieved from http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf.

³ 2012 Republican Platform. [2012]. We believe in America. Retrieved from http://www.gop.com/2012-republican-platform_We/#Item11.



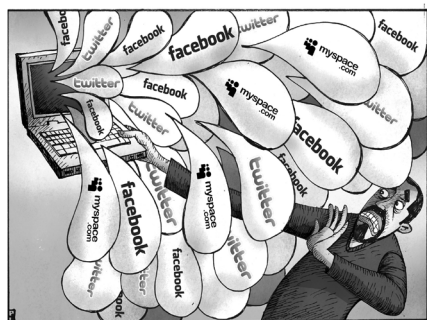
CELL PHONE LOCATION TRACKING

Cell phone geographical location can be tracked by phone companies whenever cell phones are turned on. Cell phone information can provide real time location of a person and monitor a person's movement; provide historic information on where a person has travelled; or provide collective information identifying the cell phones in an area at any given time. Law enforcement – often without a warrant – obtains real time and historic information about a person or location from a telecommunications company. **Cell phone carriers reported that they responded to 1.3 million demands for subscriber information in 2011 from law enforcement agencies seeking text messages, caller locations and other information⁴.**

In Ohio, many law enforcement agencies lack guidelines for using cell phone location tracking.

The ACLU of Ohio recommends legislation to regulate the use of cell phone location tracking in Ohio. This legislation should require:

- Warrants are obtained prior to obtaining location information.
- Retention and sharing policies are created for the information.
- Prohibition of secondary use of data.
- Explicit, written and public policies and procedures for the use of cell phone location tracking.
- Independent audits of location tracking information by law enforcement agencies.



SOCIAL MEDIA PRIVACY

In the past few years, employers and school officials have begun requesting employee, applicant, and student social networking passwords or requiring them to friend HR managers, school officials, teachers, and coaches with no privacy restrictions. Providing this access violates the privacy of the account holder as well as friends, family, clients, and anyone else with whom he or she may have communicated or shared files. Additionally, sharing access to social networking accounts may provide information about the applicant – such as age, religion, ethnicity, or pregnancy – about which an employer is forbidden to ask. This can expose an applicant to discrimination, and an employer to lawsuits from rejected job candidates claiming such discrimination.

The ACLU of Ohio recommends legislation that expressly prohibits violations of social networking privacy. This legislation should make it illegal for employers or school officials to require, request, suggest, or cause any student, employee or prospective employee to:

- Provide passwords to password-protected accounts; or
- Permit access to private material through indirect routes such as requiring employees to add them to their private social networks.

For more information on these issues visit www.acluohio.org.

⁴ Lichtblau, E. (2012, July 8). Wireless firms are flooded by requests to aid surveillance. The New York Times. Retrieved from <http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=1>.