



Connecting the Dots . . .

Surveillance in Our Society

Since September 11th, 2001, surveillance in our society has increased at an alarming rate. There has been a rapid expansion of surveillance powers, a severe reduction in judicial, congressional, and public oversight of law enforcement activities, and billions of dollars allocated to the Department of Homeland Security for the development and deployment of a new and far more intrusive surveillance infrastructure.

When you talk on the phone, open your mail, walk down the street, attend a demonstration or travel, the government wants to know about it, and they are getting the technological tools to do so.

Local, state, and federal governments claim such systems are necessary to “connect the dots” and keep us safer from terrorism. But these systems are being increasingly used to track and monitor innocent people throughout our country, with no evidence that any of it is actually making us any safer.

Now, it’s up to us to “connect the dots” on government surveillance—to educate ourselves and others, to see the big picture of parallel developments in the worlds of technology, law, and politics, and shed light on the overall danger of far-reaching government surveillance.



Listening to Our Phone Calls: In violation of federal and state laws, the National Security Agency is monitoring the calling records of every American and then listening to telephone calls without a warrant. In August 2006, a federal judge in Detroit found the warrantless eavesdropping program both unconstitutional and illegal as a result of an ACLU lawsuit. Last spring, the ACLU-NC sued AT&T and Verizon—on behalf of its 55,000 members and individuals—saying that the tele-communications giants were violating state law and regulations by illegally disclosing the call records to the NSA.

Tracking Our Travel: No Fly Lists and ATS: Since 9/11, the number of travel watch lists has mushroomed, all with very little criteria for placing names on the list, and with no effective means to remove them. It is estimated that 50,000 people are now included on the No Fly list. Two years ago, Congress barred the implementation of a more extensive domestic travel tracking program because of widespread concerns regarding inaccuracy and lack of privacy protections and instructed DHS to fix the problems. It was recently revealed that rather than following Congress’ requirements, DHS secretly deployed another program behind the backs of Congress and the American people called the Automated Tracking System (ATS). ATS matches the names of travelers against government databases to determine whether a person’s background or behavior indicates a terrorist threat, and then assigns each individual a numeric “terrorist” risk rating. You cannot see, challenge, or correct your “terrorist” risk rating or the information on which it is based and the data is maintained for 40 years and shared with local, state, and foreign governments.

Opening Our Mail: President Bush quietly issued a signing statement earlier this year in which he asserts his right to open mail without a warrant. Historically, signing statements have been used by presidents to explain how they intend to enforce the laws passed by Congress; Bush has used them to quietly assert his right to ignore those laws.

Monitoring Our Money: The CIA is secretly sifting through the records of the financial records flowing through the global financial cooperative SWIFT, without Congressional authorization or judicial oversight.

Forcing Us to Carry National ID Cards: The Real ID Act authorizes the creation of one of the most comprehensive personal databases in American history, one that lists and contained detailed information on virtually every person over age 16. It creates a national ID card and enables the government to routinely track the location and activities of individuals by forcing states to standardize their drivers' licenses, link to databases shared with every federal, state and local government agency, and storing our personal information in a uniform format that can be easily scanned by readers around the nation. Pressure against the implementation of Real ID is mounting in the states and repeal legislation has been recently introduced in Congress. For more information, please visit www.realnightmare.org.

Putting Computer Chips in IDs: Since 9/11, the government has been increasingly interested in embedding tiny computer chips called RFID tags in our identity documents. These tiny computer chips, which can be programmed with any information and then read at a distance by a reader without alerting the holder of the tag, are already in new passports and are being seriously considered by Homeland Security for more ID documents. The inclusion of RFID technology without proper privacy and security safeguards would mean that you could be tracked and monitored as you walked down the street, attended a protest, or went to the doctor's office. Landmark privacy legislation on the use of RFID in identification documents is moving through the California legislature. Visit www.aclunc.org/tech for more information.

Watching Political Activity: The Department of Defense (DOD) and consistently monitoring peaceful groups engaged in constitutional activity. Through Freedom of Information Act (FOIA) requests, the ACLU learned that the Threat and Local Observation Notice Database of the DOD contains information on numerous antiwar and counter recruitment protests, including demonstrations at UC Berkeley and UC Santa Cruz. The FBI has consistently monitored peaceful groups such as the Quakers and, of course, the ACLU.

Monitoring Where We Go and What We Do: Public Surveillance cameras are going up in cities across California and around the country. Zooming in close enough to read the title of the book you are reading and the face of the person you are talking to or hugging goodbye, they have widespread implications on privacy and the ability to engage in free speech and anonymous, lawful protest. The cameras installed today will likely become even more intrusive in the years to come, as they are paired with other new developments, such as facial recognition, iris scanning, and RFID-embedded identification documents, giving law enforcement the ability to develop dossiers about our personal lives.



More information is available at www.aclunc.org
and the Technology and Civil Liberties Page and blog at www.aclunc.org/tech