

UNCLASSIFIED  
Department of State

S/S-0  
DOTSO



UNCLASSIFIED  
Department of State

S/S-0  
OUTGDIR

SPACE 03 OF 03 STATE 215216

085/10 00222 00251

5230 081/10 00222 002  
/000 2  
RELEASABLE  
(C) EMB 70115  
S/S-0 -SPACE  
135601 1322221 /11

AS SUCH, IMPORTANT IN TRAINING OPERATIONS  
AGAINST "COMMUNIST-REVOLUTIONARIES".  
INTELLIGENT AND  
FLEXIBLE ON TACTICS, THROUGH A THOROUGHLY COMMITTED  
FUNDAMENTALIST. HE IS THOUGHT TO BE EQUALLY WELL-DISPOSED  
TO THE U.S. AND U.S.S.R.

4. THE SECOND NAME SUPPLIED BY NASHWEI WAGOOTHE  
GOSBARIYAN, IS WELL-KNOWN TO THE OSO AS A TALENTED  
FABRICATOR. HE IS THE DISTINGUISHED BY A OFFICIAL DESCRIBED

DATE  
CLASSIFIED DECLASSIFIED BY  
EXEMPT FROM E.O. 13526  
EXEMPT FROM E.O. 13526

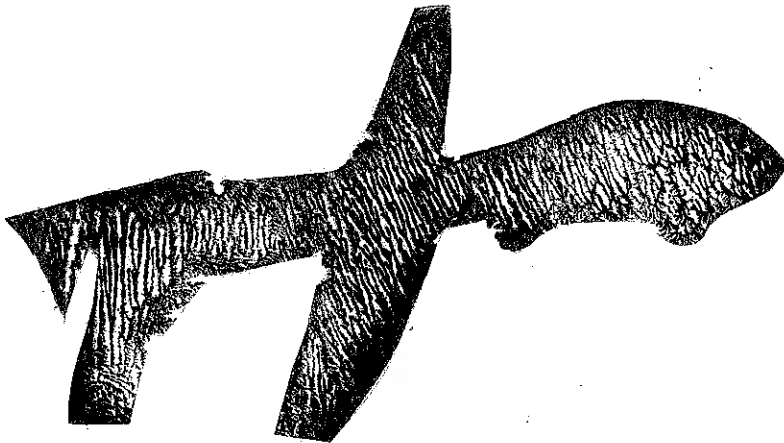
IN, #3  
ANIAN CONTA

# WE ARE ALL SUSPECTS

UNCLASSIFIED

ATIONS MAY BE  
HOW THEY RECI  
SERVICES TO  
CAN OFFICIAL  
DES BY NASHWEI  
ELDED THE FBI  
RITATIVE.

AN IMPORTANT OFFICIAL  
EXHIBIT  
MAIN ACQUIRED



CC BY-NC-SA www.creativecommons.org

This guide was created by a group of Radical Reference Librarians who are working on issues of surveillance and privacy. To get involved with our group, send an email to [alienmactina@gmail.com](mailto:alienmactina@gmail.com)

... since major [redacted] was making a position

... followed the object in a diving turn to the left descending to an altitude of about 16,000 feet with the object about 5,000 feet below and to the right of the aircraft. Thereafter he tried to keep a course parallel to the above,

a guide for people navigating the expanded powers of surveillance in the 21<sup>st</sup> Century

... as several targets as described in the attached report. ... orders that the news item reporting the observation by the fighter pilots could have caused the imaginations of the radar observers to run wild. This is considered remote in view of the number of observers witnessing the scope returns and the fact that four such incidents are reported in two days. However, the possibility is being investigated and results will be submitted upon receipt.

BRUCE K. SANDERSON  
Lt. Colonel, USAF

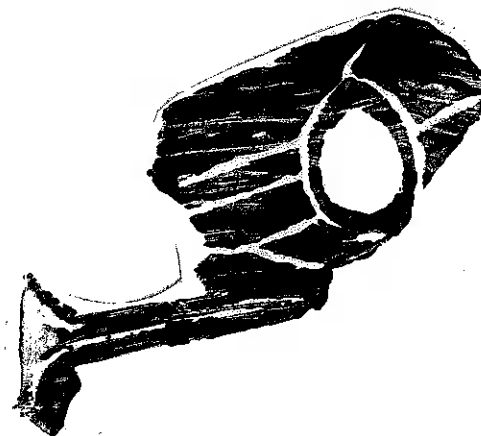
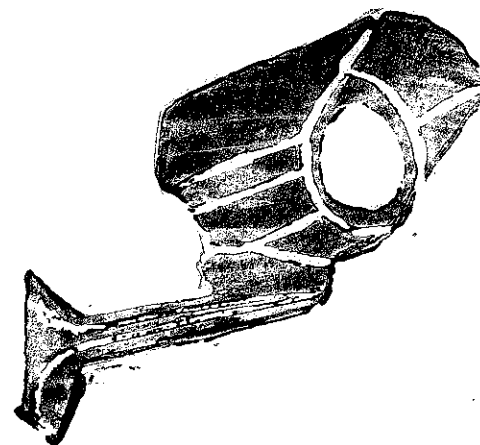
Ever since the events of September 11<sup>th</sup>, something has been happening to our privacy rights. The aftermath of this national tragedy has been an unprecedented expansion of mass surveillance in the name of "national security". Technological progress has enabled surveillance to be both ubiquitous and ultra-pervasive, seeping into all aspects of the public and private spheres. Recent revelations about dragnet surveillance prove that we are having our data collected, stored, and analyzed, even if we've been charged with no crime. In this world of mass surveillance, we are all suspects.

Librarians have always been fierce defenders of privacy. As a profession, we've opposed undemocratic and illegal threats to 1<sup>st</sup> and 4<sup>th</sup> Amendment rights from McCarthyism to the USA PATRIOT Act. It's unsurprising that these issues are of paramount importance to us; as information professionals, we know that privacy is fundamental to freedom. Even more importantly, privacy is vital to human dignity, recognized by the United Nations Universal Declaration of Human Rights. Our freedoms of association, speech, and thought all depend on our privacy.

That's why we've created this anti-surveillance, pro-privacy publication. Information and action is critical to the fight against surveillance. We hope that this publication will help.

Signed,

Your anti-surveillance Radical Reference Librarians



son of [redacted] has been there for 2 1/2 months. His investigation is finished. When asked about abuse he said his toes had been burned but it was not apparent to CSC inspection. He also said he had been kicked and beaten while blindfolded, that they had stepped on his belly. This reportedly took place in the NDS office. When asked who had abused him he said it was officers at NDS however he could not identify them due to the blindfold. NDS alleged that [redacted] had killed two ANP in Myan Shri or Shih Wai Kot before being

a/c



**DEPARTMENT OF DEFENSE**  
CRIMINAL INVESTIGATION TASK FORCE (DEPLOYED)  
QUANTANAMO BAY, CUBA

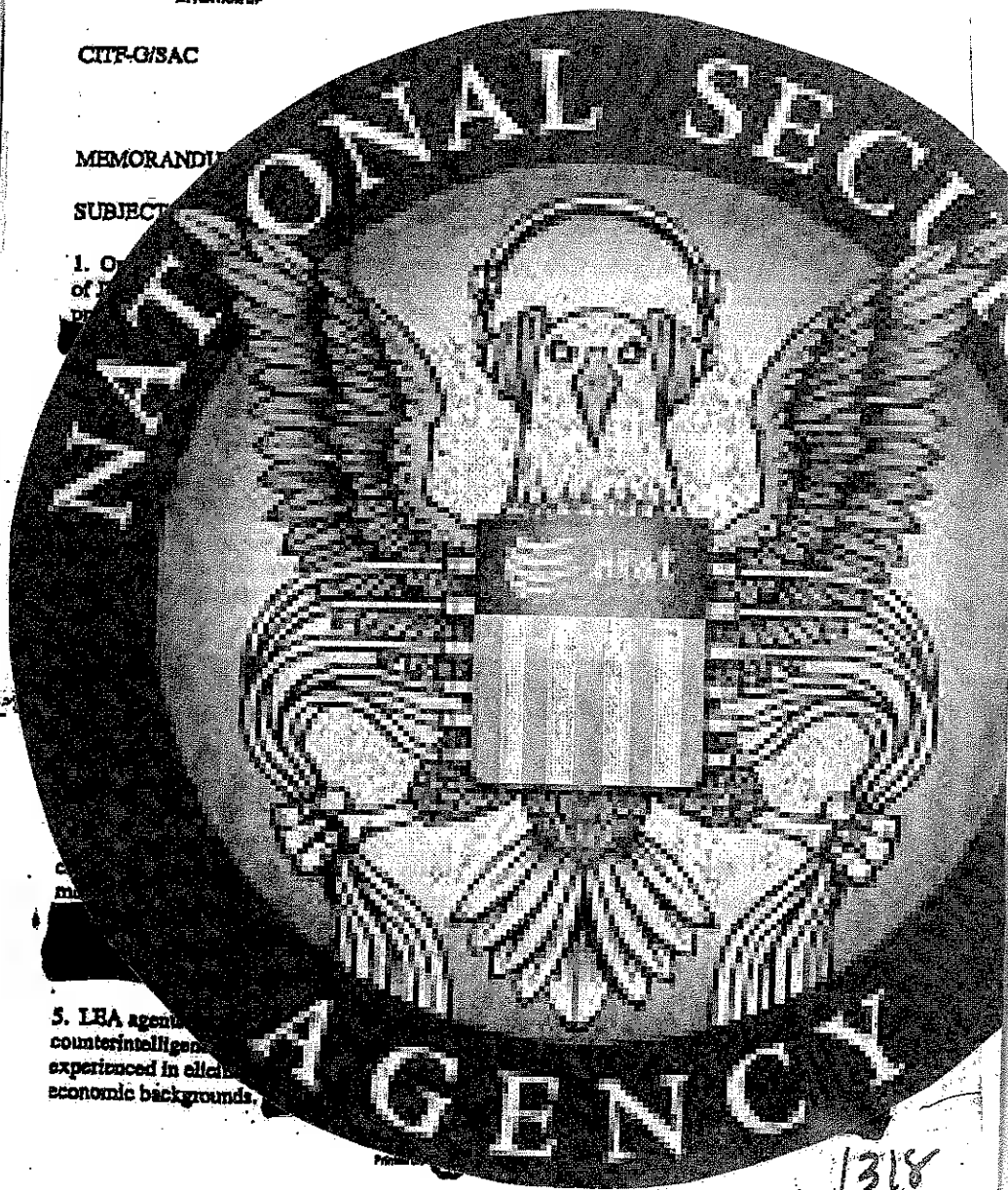
REPLY TO  
ATTENTION OF

CITF-G/SAC

MEMORANDUM

SUBJECT

1. O  
of D  
PR



5. LEA agents  
counterintelligence  
experienced in ethnic  
economic backgrounds.

1318  
PART 00102 110

**Reading list continued!**

Daniel Solove's *Nothing to Hide*.  
<http://www.worldcat.org/oclc/670481512>

Daniel Solove's *Understanding Privacy*  
<http://www.worldcat.org/oclc/163707922>

Charles J. Syke's *The End of Privacy*  
<http://www.worldcat.org/oclc/41368228>

**And a handful of web resources:**

Timeline of Snowden revelations:  
<http://america.aljazeera.com/article/s/multimedia/timeline-edward-snowden-revelations.html>

Definitive guide to NSA spying programs:  
<http://www.dailydot.com/politics/nsa-spy-prgrams-prism-fairview-blarney/>

The Guardian has been at the forefront of reporting on government surveillance. Check out their NSA files  
<http://www.theguardian.com/world/the-nsa-files>

# KNOW YOUR RIGHTS

*Congress of the United States*

The First and Fourth Amendments of the Constitution are the two amendments most often invoked when fighting for our privacy rights.

## THE FIRST AMENDMENT

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

## THE FOURTH AMENDMENT


The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.


Don't forget:  
strong passphrases  
go a long way in protecting your privacy.


ALSO:  
cover the camera on your laptop and phone!


## KEY


: encryption


: mobile


: email

: not free (or includes some fee-based services)

: prevents tracking from analytics, ads, or beacons

: browser plugins or web applications

: desktop applications or operating systems

: difficult for the average user

**Hide My Ass!:** [hidemyass.com](http://hidemyass.com)

VPN, proxy services, and other ways to securely and privately surf the web. Some free services.

**HTTPS Everywhere:** [eff.org/https-everywhere](http://eff.org/https-everywhere)  
Browser plugin that encrypts your communication on many websites.

**Mozilla Firefox:** [mozilla.org/en-us/firefox](http://mozilla.org/en-us/firefox)  
Free, open-source web browser with excellent options for privacy plugins.



**Pidgin:** [pidgin.im](http://pidgin.im)  
Free chat client with an off-the-record plugin for encryption. First, create an anonymous XMPP account ([jabber.org](http://jabber.org)).




**Silent Circle:** [silentcircle.com](http://silentcircle.com)  
A host of different encryption services for email, mobile, desktop, text, and email.





**Text Secure:** available in the Android app store  
Encrypted SMS (text message) app for Android devices only.

**Tor:** [torproject.org](http://torproject.org)  
Free software and open network that allows you to surf the web with an anonymous IP address.



Use your technology, don't let your technology use you! Encryption services, tracker-blocking, and open-source software are just some of the tools you can use to take control of your tech privacy. Here's a list of some of our favorite tools.



**Chat Secure:** chatsecure.org    
Free and open source encrypted chat client for  
iPhone or Android




**Disconnect:** disconnect.me     
Browser plugin that blocks trackers, also includes  
some encryption for communication.





**Do Not Track Me:** donottrack.me      
Browser plugin that blocks trackers with the added  
benefit of preventing your email from being  
tracked. Some free services.



**DuckDuckGo:** duckduckgo.com    
DDG is a search engine that doesn't track you. Also  
available as a Firefox plugin.

**Ghostery:** ghostery.com    
Browser plugin that blocks most invisible trackers,  
easy to toggle on and off for site functionality.

**Gnu/Linux Operating Systems:** linux.com     
Free, open-source alternatives to Windows and Mac  
OS. Ubuntu is a popular distribution.

**GnuPG:** gnupg.org      
Free software that allows you to encrypt and sign  
your email with a secure key.

What to do if law enforcement comes knocking:

-Do not consent to a search. Ask to see and read a warrant.

-Do not voluntarily hand over passwords, encryption keys, hard drives, or computers. Ask for a warrant.

-If there is a warrant, examine it carefully, and only consent to searches of the areas specifically mentioned in the warrant.

-If you are being searched, you do not have to assist. But do not obstruct or interfere with the search. You may be charged with a crime.

-You don't have to talk to the cops! You do have the right to remain silent. Be aware that anything you say can be used against you later. And don't tell any lies! You could be charged with a crime. Ask to speak with your lawyer.

ALSO: -If you do get arrested, the police may be able to search your person, your belongings, or the contents of your phone. This varies by state. Talk to your local ACLU for more info.

-Your roommate, spouse, partner, lover, or guest may have the ability to give third party consent to search on your behalf. Make sure to talk to these people about what to do if law enforcement shows up.

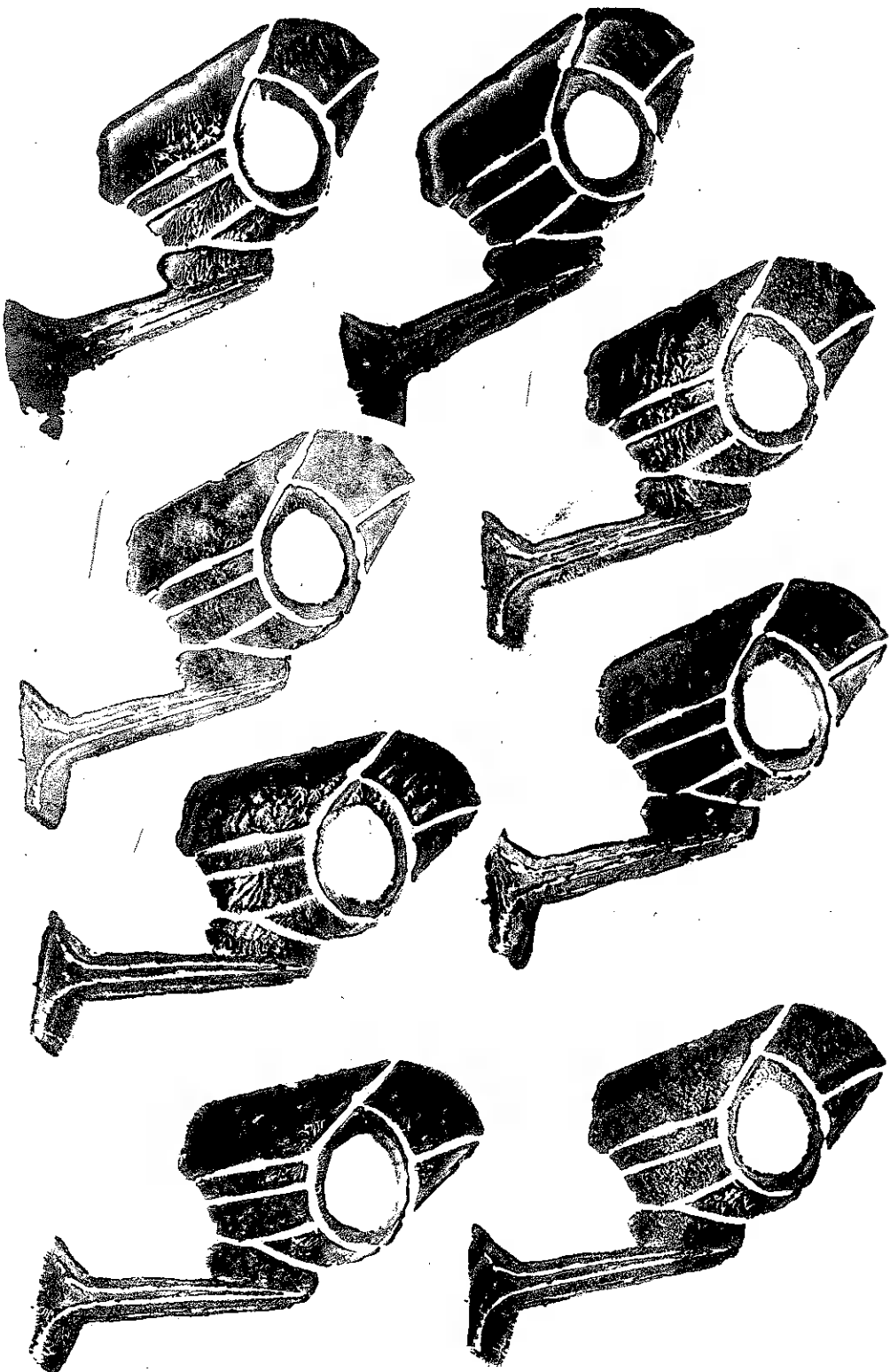
some helpful phrases when in doubt:

And don't forget: "I do not consent to a search."

"Am I free to go?" "Come back with a warrant."

"I want to speak with a lawyer."

...and take a moment to note the officer's name  
and badge number.



Pro-privacy, anti-surveillance reading list. Find them at your library using the link to WorldCat!

Ellen Alderman and Caroline Kennedy's *The Right to Privacy*  
<http://www.worldcat.org/oclc/32274009>

Simson Garfinkel's *Database Nation: The Death of Privacy in the 21<sup>st</sup> Century*  
<http://www.worldcat.org/oclc/44964667>

Evgeny Morozov's *To save everything, click here: The folly of technological solutionism.*  
<http://www.worldcat.org/oclc/778420675>

Helen Nissenbaum's *Privacy in Context.*  
<http://www.worldcat.org/oclc/436310287>

James B. Rule's *Privacy in Peril*  
<http://www.worldcat.org/oclc/126227072>

Robert Ellis Smith's *Privacy, How to Protect What's Left of It*  
<http://www.worldcat.org/oclc/4496889>



WHO IS UNDER THE MOST  
SURVEILLANCE? HISTORICALLY  
MARGINALIZED PEOPLE, INCLUDING:

PEOPLE OF COLOR

MUSLIM-AMERICANS

IMMIGRANTS

ACTIVISTS

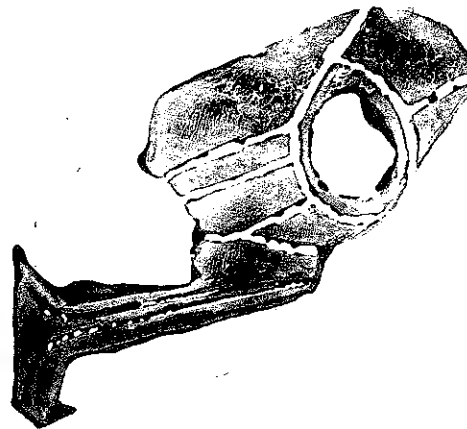
POLITICAL DISSIDENTS

QUEER AND TRANS\* PEOPLE

PEOPLE LIVING IN POVERTY

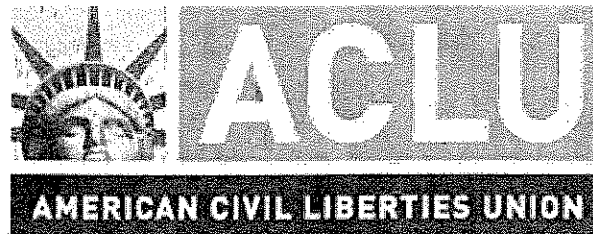
PEOPLE WHO ARE HOMELESS

PEOPLE WHO ARE IN OR HAVE  
BEEN TO PRISON



*for legal  
assistance or  
more information,  
contact*

↙ ↘



American Civil Liberties Union

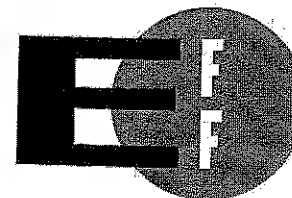
[www.aclu.org](http://www.aclu.org)

(212) 549-2500

National Lawyers Guild

[www.nlg.org](http://www.nlg.org)

(212) 679-5100



Electronic Frontier Foundation

[www.eff.org](http://www.eff.org)

(415) 436-9333

AT&T WIRELESS

The NSA collects huge volumes of transactional metadata, such as credit-card purchases, bank transfers, and web addresses. Metadata includes information like time and location of the transaction. It can tell a lot about who you are, where you're going, and what you're doing.

*Some of the ways you are being spied on and tracked.*

### MOBILE PHONES

Just by carrying your mobile phone and leaving on location services, wifi, or Bluetooth, you are able to be tracked. Other kinds of data on your phone are also being collected: documents leaked by Edward Snowden show that the NSA collects 5 billion cell phone records each day. By tapping into mobile network data, the NSA collects location information, call records, and SMS texts. NSA implants can take over mobile phones and control them remotely.

### AERIAL SURVEILLANCE

Another major DHS initiative, aerial surveillance usually comes from spy drones (unmanned aircraft equipped with sensors to detect objects at high-resolution from great distances). Drone technology is so advanced that some of these vehicles are as small as Humvees.



**james clapper**  
such spy  
director of national intelligence  
very counterterrorism

### SURVEILLANCE CAMERAS

The use of these cameras, by both law enforcement and businesses, has increased dramatically. Department of Homeland Security grants provide billions each year for various Homeland Security agencies to install even more cameras. Look up—you'll spot one.

**j. edgar hoover**  
longtime director of the FBI  
very spy  
such cointelpro

### BIOMETRICS

Biometric data is used to identify people by physical characteristics. Facial recognition, fingerprints and DNA are some examples of this data. Law enforcement agencies are amassing an enormous biometric database; likewise, Facebook owns one of the largest facial recognition databases.

**wow general keith alexander**  
former director of the NSA  
much spying on you  
so prism

### TELEPHONE DATA

The two largest telecoms, Verizon and AT&T, are paid huge sums by law enforcement agencies for access to bulk call records. All telecoms are required by the Communications Assistance for Law Enforcement Act to allow wiretapping by law enforcement.

### COMPUTER SURVEILLANCE

Law enforcement and national security agencies have the ability to monitor, store, and analyze all internet traffic. Surveillance computers employed by these agencies can look for keywords that signal so-called suspicious behavior. These agencies also have the ability to install spyware to remotely monitor the

