a guide for people navigating the expanded powers of surveillance in the 21st century

This guide was created by a group of radical surveillance activists working on privacy. To get involved with our group, send an email to disinformation@ow.com

www.creativecommons.org
Ever since the events of September 11th, 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 1st and 4th 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
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:  

Definitive guide to NSA spying programs:  

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
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.

KEY
ADS: prevents tracking from analytics, ads, or beacons
encryption
mobile
email
desktop applications or operating systems
not-free (or includes some fee-based services)
difficult for the average user

Hide My Ass!: hidemyass.com
VPN, proxy services, and other ways to securely and privately surf the web. Some free services.

HTTPS Everywhere: eff.org/https-everywhere
Browser plugin that encrypts your communication on many websites.

Mozilla Firefox: mozilla.org/en-us/firefox
Free, open-source web browser with excellent options for privacy plugins.

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

Silent Circle: 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
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 MacOS. 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: 
“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 21st 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
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.

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.

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.

ERIAL SURVEILLANCE

Another major DHS initiative, erial surveillance usually comes from drone surveillance, 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 bumblebees.

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.

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