Know Your Rights

Everyone has basic rights under the U.S. Constitution and civil rights laws. It is important to understand your legal rights when dealing with the police and other government officials. However, you cannot assume officers will behave in a way that protects your safety or that they will respect your rights even after you assert them. The police may “read you your rights”, but they also do everything possible to get you to waive these rights. Never Waive Any of Your Rights!

According to the ACLU, when dealing with the police… You Have The Right To:

ASK IF YOU ARE FREE TO LEAVE. If the answer is yes, DO IT! Not every encounter with police is a “stop” and you may be free to just walk away.

REMAIN SILENT. Seriously, you don’t have to talk! You can say, “I’m exercising my right to remain silent” and then don’t speak.

RECORD the interaction, but be aware that holding or reaching for a mobile device may be viewed as threatening.

ASK FOR A LAWYER immediately if you are arrested or taken to a police station. You don’t have to know a lawyer; you can ask for information to call one and they must provide it.

DECLINE A REQUEST TO SEARCH your car, your home, your belongings, or your person.

Calmly say “I do not consent to a search.”

- A warrant-less search is allowed in some circumstances, but it is always helpful to say you don’t consent to a search.

- An officer can pat you down if they suspect a weapon.

- An officer can require that you show your ID if you are driving a car or in certain cases involving alcohol or marijuana.

- An officer must have a warrant to enter your home unless they are responding to an emergency.

Download Know Your Rights guides from the ACLU of Washington. [https://www.aclu-wa.org/know-your-rights](https://www.aclu-wa.org/know-your-rights) If you are in a different search for the ACLU Know Your Rights guide for your state.

The National Lawyer’s Guild has a similar Know Your Rights guide. Download and read this guide as well. [https://www.nlg.org/know-your-rights/](https://www.nlg.org/know-your-rights/)

Although several years old (2008), the Don’t Talk to the Police presentation by Regent University School of Law Professor James Duane is essential for understanding your rights in an encounter with the police. Professor Duane gives viewers startling reasons why you should always exercise your 5th Amendment rights when questioned by government officials. The presentation is available on YouTube. [https://www.youtube.com/watch?v=d-7o9xYp7eE](https://www.youtube.com/watch?v=d-7o9xYp7eE)
Some people believe that failure to talk to the police and requesting a lawyer if you are detained by the police somehow means that you are guilty of a crime or have something to hide. However, this is definitely not the case. Your right to remain silent, and your right to legal counsel is intended to protect the innocent from police and government abuses. In Ohio v. Reiner, 532 US 17, 20 (2001) the US Supreme Court said: “One of the Fifth Amendment’s basic functions is to protect innocent men who otherwise might be ensnared by ambiguous circumstances... Truthful responses from an innocent witness, as well as those of a wrongdoer, may provide the government with incriminating evidence from the speaker’s own mouth.”

You must never make any statement to the police. Even the most truthful and innocent statement can be used to bring criminal charges against you. U.S. Supreme Court Justice Stephen Breyer, writing in Rubin v. United States 524 U.S. 1301 (1998) stated: “The complexity of modern federal criminal law, codified in several thousand sections of the United States Code and the virtually infinite variety of factual circumstances that might trigger an investigation into a possible violation of the law, make it difficult for anyone to know, in advance, just when a particular set of statements might later appear (to a prosecutor) to be relevant to some such investigation.”

Supreme Court Justice Robert Jackson, writing in Watts v. Indiana, 338 U.S. 49 (1949) stated: “Any lawyer worth his salt will tell the suspect in no uncertain terms to make no statement to the police under any circumstances.”

The Police Can Lie to You and They Will Lie About You

While it is illegal for you to give a false statement to the police (lie), it is not illegal for the police to lie to you. In fact the police will routinely lie to suspects in order to gain their cooperation or get them to confess to a crime. Although it has been repeatedly shown that police dishonesty has negative consequences for innocent individuals suspected of a crime and may push them into confessing or pleading guilty to an offense that they had nothing to do with; police continue to lie to and mislead suspects in order to get convictions. Not only will the police lie to you, they will lie about you!

Norm Stamper, a former Chief of Police for Seattle, WA, wrote in his book To Protect and Serve: How to Fix America’s Police, “For anyone who has practiced criminal law in the state or Federal courts, the disclosure about rampant police perjury cannot possibly come as a surprise. “Testilying” – as the police call it – has long been an open secret among prosecutors, defense lawyers, and judges.” Stamper continued, “In my professional experience, there are too many cops who become habituated to lying... Even as they put innocent people behind bars, or in the ground.”

“Sadly, deception is all but robotic in many police departments...” wrote Stamper. It is an all too common practice for police to lie in their testimony to the courts, in probable cause statements used to obtain warrants, and in their investigative reports forwarded to the prosecutor. Even if the police don’t intentionally lie, they can misinterpret, make inaccurate reports, or fail to include exculpatory information. The law requires that exculpatory information be disclosed to defense counsel in a criminal case (See: Brady v. Maryland: 373 U.S. 83 (1963)), but the police can easily “lose” information that does not support the charges they are trying to make against you.

In an article in the Los Angeles Times (February 11, 1996), Joseph McNamara, a former Chief of Police in both Kansas City and San Jose, stated: “As someone who spent 35 years wearing a police
uniform, I’ve come to believe that hundreds of thousands of law enforcement officers commit felony perjury every year [when] testifying…”

It is clear that you cannot trust the police to always tell the truth or to write accurate and unbiased reports. Furthermore, government agencies can use their police powers to target and harass anyone. As a police commander at Joint Base Lewis-McChord (JBLM) in Washington State once said “You don’t have to actually have done anything wrong, we just have to make it look like you did.” Even if the police don’t win their case in court, they can and do use bogus citations as a means of harassment and retaliation.

In his book A Toast to Silence, Peter Baskin, an attorney with more than 50 years’ experience, wrote that the police method “consists of the universally recognized and approved practice of deception, manipulation, misrepresentation, and any and every trick, tactic and seductive lie in order to get people to talk and give evidence against themselves”. Regent Law School Professor James Duane wrote in his book You Have the Right to Remain Innocent: “Do not think for a minute that you can trust a police officer who seems to be open minded and undecided about whether he will arrest you after you are finished with an “interview” – the police are trained to act that way, to get you to talk with them for many hours until you finally give up in exhaustion.” Laura Coates, CNN Legal Analyst and former Assistant United States Attorney for the District of Columbia wrote in her book You Have the Right: “A police officer can try to trick you or lie to you or mislead you to get you to confess something…”

Countermeasures Against Police and Government Corruption

The Electronic Frontier Foundation (EFF) in an article **Know Your Rights** (2014) stated: “Your computer, phone, and other digital devices hold vast amounts of personal information about you and your family. This sensitive data is worth protecting from prying eyes, including those of the government... The Fourth Amendment to the U.S. Constitution protects you from unreasonable government searches and seizures, and this protection extends to your computer and portable devices. But how does this work in the real world? What should you do if the police or other law enforcement officers show up at your door and want to search your computer?” [https://www.eff.org/issues/know-your-rights](https://www.eff.org/issues/know-your-rights) This article can help you understand your rights in the digital world, and the **EFF Surveillance Self-Defense** page [https://ssd.eff.org/](https://ssd.eff.org/) will provide you with tools to protect yourself against police corruption.

To limit interception of your communications it is essential that you protect the content of your messages with end-to-end encryption, using apps such as Signal [https://signal.org/](https://signal.org/), Wickr [https://wickr.com/](https://wickr.com/), and Viber [https://www.viber.com/](https://www.viber.com/). Use these apps to communicate securely with people that you trust. To have secure end-to-end communication everyone must be using the same app. We ruled out some of the most popular messaging apps (in particular, Whatsapp and Facebook Messenger) because of their ties to major tech companies. Between their data security problems, their political biases, and the pressure they face from law enforcement to break the encryption on their products, we think you should look elsewhere for secure messaging. [https://blokt.com/guides/most-secure-messaging-apps](https://blokt.com/guides/most-secure-messaging-apps)

E-mail should also be end-to-end encrypted. While encryption protects the content of your e-mail, metadata such as the addressees of a message, the date and time messages are sent, and like data for e-mail received is not protected by encryption. It is therefore useful to choose an e-mail provider that is located outside your country of residence, thereby limiting the ability of government officials to use
subpoenas to obtain copies of your e-mail records. Protonmail [https://protonmail.com/], located in Switzerland and Tutanota [https://www.tutanota.com/], located in Germany are examples of very popular encrypted e-mail services.

Even when using an encrypted e-mail service, you should use two-factor authentication to increase the security of your on-line accounts. When an account is protected with two-factor authentication a login token is required along with your username and password in order to access your account. This token may be a number sent as a text message to your cell-phone, or an number created by an app, such as Google Authenticator. In this way even if someone determines your password, that person must still have access to your cell-phone in order to complete the login. (In 2018, the Computer Systems Administrator in the Joint Base Lewis-McChord (JBLM) Directorate of Emergency Services (DES) was able to obtain the passwords of the personal e-mail accounts of individuals being targeted and harassed by JBLM. The Systems Administrator then illegally accessed the personal (non-government) e-mails of those individuals.)

Use Blind Carbon Copy (BCC) when sending e-mail. Even if a corrupt government agency cannot read the content of your e-mail (because it’s encrypted), information can still be obtained from the header of your e-mail. By putting addressees of your message on the BCC line, instead of the To line of an e-mail, someone obtaining a copy of that e-mail cannot see everyone you are communicating with.

According to court documents, the Joint Base Lewis-McChord (JBLM) Protection Division obtained information (and identified members) of political groups, such as the Olympia Movement for Justice and Peace (OMJP) by signing up for their e-mail distribution lists and exchanging e-mail with group members.

“At the end of August 2015, it was reported that the Joint Base Lewis-McChord Force Protection Division was using Stingray cellphone monitoring devices to collect information about local political activists. Thomas Rudd, the chief of the Joint Base Lewis-McChord Force Protection Division admitted
to using the email address portwatcher[at]Hotmail.com (among others) to gain access to private list servers and collect information about political demonstrations, and to intercept privileged communications between attorneys and their clients. Even after being order to stop this electronic monitoring, Rudd stated in a 2014 deposition that he continued to illegally monitor the communications of local political groups and activists who opposed government policies.” https://www.indybay.org/newsitems/2017/03/08/18797170.php

Protect the content of your computer with full-disk encryption, using programs such as BitLocker, FileVault, or VeraCrypt https://www.veracrypt.fr/en/Home.html. Ensure that any devices that you carry with you are encrypted and secured with a strong pass-phrase. Remember that the police can force you to give up biometrics (i.e. open a locked device with your fingerprint), but they cannot legally force you to disclose the content of your mind – a memorized password.

You can also create encrypted archives with programs like 7-Zip https://www.7-zip.org/. Combined with a strong pass-phrase these encrypted archives can protect sensitive files on your computer.

7-Zip encrypted archives can be used to send encrypted messages. You can of course just place your message inside of an encrypted archive and e-mail it as an attachment, but additional security for your message can be obtained by using a file transfer program such as Swiss Transfer (Switzerland) https://www.swisstransfer.com/en, or Transfer Now (France) https://www.transfernow.net/en/.

Corrupt government agents can access everything that you post on-line and even hack into your private accounts to gain information about you or plant evidence against you. You should always access the Internet through a Virtual Private Network (VPN), using The Onion Router (TOR) https://www.torproject.org/, or through an anonymous proxy. The Amnesic Incognito Live System (TAILS) https://tails.boum.org/ is a portable operating system that protects against surveillance and censorship.

**Don’t Disclose Your Cell-Phone Number**

Your cell-phone works as a tracking device. At a minimum your general location can be determined by triangulation from the cellular towers / sites that your phone connect to. If your cell-phone is equipped with GPS it may be possible to determine your exact location based on GPS coordinates transmitted by your phone.

One option to limit the ability to track you through your cell-phone is to establish a Google Voice https://voice.google.com number. Whenever you must provide your telephone number, provide your Google Voice number. You will be able to make and receive calls and text messages and have voice mail through the Google Voice app, but you won’t be directly tracked through this number.

**Don’t take your cell-phone to any place were you don’t want to be identified.** In a February 2015 presentation, Police Surveillance and How to Avoid It, made to the Association of Alternative Newspapers/The Media Coalition Joint Conference in San Francisco; Eva Galperin of the Electronic Frontier Foundation warned of police use of cell-site simulators, called “Stingray”. A Stingray mimics a cell-phone tower and forces all nearby mobile phones or devices to connect to it. Every phone that connects to the Stingray reports its number, GPS location, and the numbers of all outgoing calls and texts. That’s every location and outgoing call and text log of every phone within a certain radius—up to several kilometers—of the Stingray.
In a January 2019 motion for a protection order to prohibit the release of information to the public and the press, Joint Base Lewis-McChord (JBLM) expressed a concern about public disclosure of information alleging that Anti-Terrorism Officers in the JBLM Directorate of Emergency Services (DES) “were using Stingray, electronic warfare equipment, to unlawfully spy on citizens.”

https://pacer.uscourts.gov/ (Note that JBLM’s use of Stingray devices to illegally monitor civilian communications had been reported as early as 2015.)

Entrapment

Entrapment is a practice whereby a law enforcement agent or agent of the state induces a person to commit a “crime” that the person would have otherwise been unlikely or unwilling to commit. It “is the conception and planning of an offense by an officer or agent, and the procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion or fraud of the officer or state agent.”

Entrapment is a complete defense to a criminal charge, on the theory that "Government agents may not originate a criminal design, implant in an innocent person's mind the disposition to commit a criminal act, and then induce commission of the crime so that the Government may prosecute." Jacobson v. United States, 503 U.S. 540, 548 (1992). A valid entrapment defense has two related elements: government inducement of the crime, and the defendant's lack of predisposition to engage in the criminal conduct. Mathews v. United States, 485 U.S. 58, 63 (1988). Of the two elements, predisposition is by far the more important. https://www.justice.gov/archives/jm/criminal-resource-manual-645-entrapment-elements

Beware of Government Spies

A search of your electronic life is not your only concern. Government agents can infiltrate private, political, and activist organizations. We saw an example of this illegal infiltration of these organizations in the case of Panagacos v. Towner, 782 F.Supp.2d 1183, 1191 (W.D. Wash. 2011) where personnel from the Joint Base Lewis-McChord Protection Division’s Anti-Terrorism Office, in Washington state, infiltrated organizations opposed to the war in Iraq.

https://www.indybay.org/newsitems/2017/03/11/18797318.php

According to an article in the Olympian Newspaper, Ex-worker at JBLM Collected Activist Data, (January 25, 2011) https://www.theolympian.com/news/local/article25280662.html “A former Joint Base Lewis-McChord employee who spied on war protests in Olympia helped compile detailed information on protesters, including their names, photos, addresses and, in some cases, Social Security numbers, according to 133 pages of law enforcement records released by the City of Tacoma.” The documents detail years of surveillance of protest groups by Joint Base Lewis-McChord and the South Sound Regional Intelligence Group. The detailed information collected about the protesters continues to be stored by area law enforcement agencies to this very day.

In 2020, personnel from Joint Base Lewis-McChord (JBLM) were reported to have infiltrated Black Lives Matter (BLM) and ANTIFA groups in Washington and Oregon. JBLM informants were able to provide information to the FBI which ultimately resulted in the arrest of a protester who had committed arson by burning two police vehicles during a Seattle BLM protest. Of course, JBLM has no lawful
Famed freedom author Claire Wolfe has stated: “These days, law enforcement at all levels -- from the local cop shop to obscure federal agencies -- uses snitches to trap ordinary people. Snitches tell lies that send their friends to jail. Paid agents provocateurs talk or trick otherwise harmless people into committing crimes. In many places, Snitch culture has virtually replaced real investigation of real crimes. Don’t think you’re exempt if you’re a "law-abiding citizen." The most trusting, naive, innocent people often make the easiest targets for these weaselly, lying, opportunistic vermin. Snitches specialize in targeting the vulnerable.” To help you protect yourself against government informers, Claire Wolfe has provided a free guide, Rats! Your Guide to Protecting Yourself Against Snitches, Informers, Informants, Agents Provocateurs, Narcos, Finks, and Similar Vermin. http://www.rats-nosnitch.com/

You’re a Homegrown Violent Extremist / Domestic Terrorist if You Question The Government

When some government agent obtains information about you, they may enter that information into a system called eGuardian https://www.fbi.gov/resources/law-enforcement/eguardian. The information entered into eGuardian is migrated to the FBI’s internal Guardian system, where it is assigned to the appropriate Joint Terrorism Task Force (JTTF) for any further investigative action. A significant problem with the eGuardian system is that the information entered into the system often lacks probable cause, or even a reasonable suspicion of criminal activity. Agencies with access to eGuardian can enter false or misleading information into the system, creating government records on American citizens who have done nothing wrong. These citizens may then be contacted and intimidated by JTTF agents based on the information entered into eGuardian.

JBLM anti-terrorism officers also collect information about U.S. Persons and enter that information into other databases and systems of records, such as Intelink https://en.wikipedia.org/wiki/Intelink and JARVISS https://jarviss.army.mil/Splash/. JBLM admitted to entering information about individuals who question government policy into these systems, only after it was reported by independent media in 2017 https://www.indybay.org/newsitems/2017/07/08/18800691.php.

A June 12, 2020 article in The Intercept reported that individuals in Cookeville, TN who posted about Black Lives Matter (BLM) demonstrations on social media were contacted and harassed by the JTTF. “What the JTTF is doing is shocking, but we saw this happen before during the McCarthy era, when the FBI and other various agencies investigated activists with the purpose of discouraging or chilling free speech,” said Will York, an attorney who specializes in free speech cases and is a founding member of the National Lawyers Guild’s Nashville chapter. https://theintercept.com/2020/06/12/fbi-jttf-protests-activists-cookeville-tennessee/

CAIR California wrote: Using JTTFs to Investigate Protesters: What You Need to Know - On Sunday, May 31, the U.S. Department of Justice (DOJ) announced that they will use the Federal Bureau of Investigation’s (FBI) 56 nationwide Joint Terrorism Task Forces (JTTF) to investigate “violence instigated by Antifa and other similar groups” under domestic terrorism laws. This announcement is likely to lead to increased surveillance, harassment and arrests of protesters by local and federal law enforcement agencies, particularly Black organizers fighting for justice and accountability. https://ca.cair.com/sfba/updates/using-jtffs-to-investigate-protesters-what-you-need-to-know/
The ACLU wrote: **New documents confirm: FBI’s Joint Terrorism Task Force targets peaceful activists for harassment, political surveillance** - The American Civil Liberties Union of Colorado released documents today that it says confirm that the FBI’s Joint Terrorism Task Force (JTTF) in Denver is targeting peaceful political activists for harassment and building files on constitutionally-protected political activities and associations that have nothing to do with terrorism or other criminal activity. [https://aclu-co.org/new-documents-confirm-fbis-joint-terrorism-task-force-targets-peaceful-activists-for-harassment-political-surveillance/](https://aclu-co.org/new-documents-confirm-fbis-joint-terrorism-task-force-targets-peaceful-activists-for-harassment-political-surveillance/)

In July 2020 we saw Joint Base Lewis-McChord (JBLM) enter fraudulent information into eGuardian in order to use the JTTF to harass and intimidate individuals in the community who had complained to the Base Commander about misconduct by personnel in the JBLM Anti-Terrorism Office (JBLMATO), and within the base’s Directorate of Emergency Services (DES).

Harassment by the JTTF at the behest of the JBLMATO is just a small part of questionable conduct being engaged in by JBLM personnel. Throughout 2019 and 2020 a notice was posted in the civilian community claiming that businesses were being placed under surveillance by JBLM because they had posted ‘anti-DOD’ fliers. [http://portland.indymedia.org/en/2020/02/438207.shtml](http://portland.indymedia.org/en/2020/02/438207.shtml)

The JTTF along with other law enforcement units and government agencies may engage in surveillance of individuals and groups that they deem to be a ‘security threat’. The following photo shows a surveillance camera mounted on a utility pole outside of a home in Tacoma, WA. The surveillance camera was used to record the activities of political activists who opposed the war in Iraq and Afghanistan. [https://www.indybay.org/newsitems/2008/07/10/18515172.php](https://www.indybay.org/newsitems/2008/07/10/18515172.php)
This video surveillance was conducted based on information provided by Joint Base Lewis-McChord (at that time Fort Lewis) anti-terrorism personnel, and was part of the illegal surveillance identified in the Panagacos v. Towery lawsuit against the government.

While casual observations of a person's forays in and out of her home do not usually fall within the Fourth Amendment's protections, the US Supreme Court has held that this type of video surveillance of a person's home does violate the Fourth Amendment.

The Court found that “A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'” [...] What's more, the Supreme Court recognized that long-term tracking of a person's movements "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.” [https://www.techdirt.com/articles/20190609/10585442362/federal-court-eight-months-utility-pole-camera-surveillance-is-fourth-amendment-violation.shtml]
Fusion Centers, Regional Intelligence Groups, and InfraGard

The JTTF along with other police and government agencies work with the Fusion Centers and Regional Intelligence Groups. Each state and many major metropolitan area have a Fusion Center https://nfcausa.org/ that gathers and disseminates “intelligence” about activities in its area. Regional Intelligence Groups work in smaller geographic areas, doing much the same thing as the Fusion Centers.

Many of the people working in the Regional Intelligence Groups are also Fusion Liaison Officers (FLO) http://wsfc.wa.gov/FLO for their state Fusion Center. InfraGard https://www.infragard.org/ is “a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure. With thousands of vetted members nationally, InfraGard's membership includes business executives, entrepreneurs, military and government officials, computer professionals, academia and state and local law enforcement; each dedicated to contributing industry specific insight and advancing national security.”

Each of these groups collects “suspicious activity reports” and creates files and records about the activities of American citizens. A major concern with this data collection and dissemination is that the information entered into these records is seldom properly vetted for accuracy, and too often is based on reporting of Constitutionally protected activities.

Automated License Plate Readers (ALPRs)

Automated license plate readers (ALPRs) are high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police squad cars. ALPRs automatically capture all license plate numbers that come into view, along with the location, date, and time. The data, which includes photographs of the vehicle and sometimes its driver and passengers, is then uploaded to a central server.

The EFF has stated: “Taken in the aggregate, ALPR data can paint an intimate portrait of a driver’s life and even chill First Amendment protected activity. ALPR technology can be used to target drivers who visit sensitive places such as health centers, immigration clinics, gun shops, union halls, protests, or centers of religious worship. Drivers have no control over whether their vehicle displays a license plate because the government requires all car, truck, and motorcycle drivers to display license plates in public view. So it’s particularly disturbing that automatic license plate readers are used to track and record the movements of millions of ordinary people, even though the overwhelming majority are not connected to a crime.” https://www.eff.org/pages/automated-license-plate-readers-alpr

Guidelines for the use of ALPRs in Washington State can be found at: https://www.waspc.org/assets/ProfessionalServices/modelpolicies/alprpolicy.pdf
Physical Surveillance

Physical surveillance – having people following you and recording your activities – is less common than other means of monitoring your activities, but it does happen. Physical surveillance is most likely to be conducted occasionally against persons of interest, rather than continuously.

Detecting and defeating a professional surveillance team, such as the FBI Surveillance Group, [https://www.fbijobs.gov/career-paths/surveillance](https://www.fbijobs.gov/career-paths/surveillance) can be extremely difficult, even for someone trained in counter-surveillance techniques. However, in most cases you will not be targeted by national level surveillance assets. State and local surveillance operations will usually involve personnel who have had some training in surveillance, but who are not full-time surveillance specialists.

Regardless of the type of surveillance team, you can make their job much more difficult if you:

- Vary your daily routes of travel. Don’t take the same route to and from work each day.
- Vary your arrival and departure times. Don’t be predictable in your comings and goings.


Police surveillance is not just about gathering evidence of criminal activity. Police surveillance is also a form of harassment used against an individual in a malicious attempt to reduce the quality of a person’s life so they will: have a nervous break-down, become imprisoned, institutionalized, experience constant mental, emotional, or physical pain, become homeless, and/or commit suicide. Harassment of this type is common when the government is targeting political opponents and activists.

Heidi Boghosian, the former director of the National Lawyers’ Guild, wrote in her book, *Spying on Democracy*: “A civilian employee of the Fort Lewis Force Protection Division in Washington State struck up friendships with many peace activists. For at least two years, he posed as an activist with Port Militarization Resistance (PMR), a group in Washington opposing the Iraq and Afghanistan invasions. He gave information about planned protests to his supervisor…, who wrote threat assessments that local law enforcement officials used in harassment campaigns that included “preemptive arrests and physical attacks on peaceful demonstrations, as well as other harassment”. One individual was arrested so many times that his landlord evicted him... In the words of the government agencies involved, they aimed to neutralize PMR through a pattern of false arrests and detentions, attacks on homes and friendships, and attempting to impede members from peacefully assembling and demonstrating anywhere, at any time. Harassment was systematic and pervasive. PMR participants were arrested not just locally, but in other venues, including the Denver Democratic National Convention in 2008 and a San Francisco protest at which they were the only ones arrested... The case revealed that today’s military has continued to engage in COINTELPRO-type operations and shows the extent to which the lines between the military and civilian law enforcement have blurred. Forces now used against ordinary people engaged in free speech and protest include, increasingly, weapons and tactics used by the U.S. military for combat missions. The drift from passive intelligence gathering to offensive counterintelligence is one manifestation of the difference between civilian law enforcement principles and the military’s exclusive focus on defeating perceived enemies...
through combat, propaganda, and covert operations... The role of civilian law enforcement, in theory, is to protect the public and the Constitution whereas the role of the military is to identify the enemy and neutralize them... When the military starts identifying peaceful dissenters here as the enemy, God help us all.” (Boghosian 2013, 107-108)

### Trash Analysis

Trash Analysis is a technique employed by law enforcement where they literally go through a suspect's garbage, looking for potential evidence of criminal activity or to verify the identification of the residents via “indicia of residency” such as utility bills, etc.

When you place your trash alongside the curb, it is considered abandoned and fair game for others to examine. Under the law, when it comes to searches, police can’t violate your Fourth Amendment rights when you have no reasonable expectation of privacy in the place or thing being searched. The Supreme Court has held that garbage cans constitute “abandoned property” and the individual loses any privacy interest or standing to challenge the search.

A mere hunch is sufficient to justify a trash analysis. Hearsay, rumor and innuendo can be enough to pique police interest in one’s trash. Anything incriminating the police find can be used by law enforcement to secure a search warrant for the premises from which the trash originated.

So keep this in mind the next time you think about throwing anything away, especially if it’s something you wouldn’t want police seeing.

### Drug Dogs

The accuracy of drug dogs is less accurate than a coin flip. NPR (2011) reported that “Drug-Sniffing Dogs Are Wrong More Often Than Right”.

A 2011 study by the University of California Davis (UC Davis) found that “Explosive- and drug-sniffing dogs' performance is affected by their handlers' beliefs”.

A 2019 report by the Washington Post found that “Multiple analyses of drug-dog alerts have consistently shown alarmingly high error rates — with some close to and exceeding 50 percent. In effect, some of these K-9 units are worse than a coin flip.”

### What Can You Do?

You Can Photograph / Video The Police

Almost every court to consider the issue has determined that the First Amendment gives you the right to record (pictures, video, and audio) police officers in public while they are performing their duties. But that doesn’t mean you’re allowed to record if you’re doing so surreptitiously (secretly), interfering with the officer, or otherwise breaking the law.

The courts’ primary rationale for allowing police officer recording is that the First Amendment includes the right to freely discuss our government, and the right of freedom of the press and public access to information. Given the prevalence of personal filming devices, more and more “news” is being gathered and disseminated by members of the public. The courts have found that freedom of the press applies to citizen journalists and documentarians just as it does to formal members of the press. (See: Glik v. Cunniffe, 655 F.3d 78 (1st Cir. 2011))

The First Amendment means police will have to endure some amount of observation and public, verbal challenge. Likewise, they must endure the critical, documentary eye of a recording. However, they don’t have to endure the act of recording if it interferes with their ability to do their jobs. (City of Houston v. Hill, 482 U.S. 451(1987); Glik v. Cunniffe, supra.)

Uniformed officers may legitimately order citizens to cease recording if the recording is interfering with or obstructing their law enforcement duties. You might be obstructing an officer (and thereby committing a crime) if, for example, you are standing close to him while he is attempting to arrest someone and your recording is clearly provoking the arrestee or other bystanders to become hostile or violent. (Gericke v. Begin, 753 F. 3d 1 (1st Cir. 2014); Glik v. Cunniffe, supra.)

If the police retaliate against you for recording them, you might or might not have a good lawsuit. You could have a case against them under a federal law, 42 U.S.C. § 1983 (“section 1983”), for deprivation of civil rights. Your claim might involve your First Amendment right to record and your Fourth Amendment right against unlawful arrest.

An example of police retaliation against a photographer can be seen in these YouTube videos, wherein a Military Police (MP) Officer assaults a person filming the Dupont Gate of Joint Base Lewis McChord from off-post:

Joint Base Lewis McChord- 1A Audit (Pt. 1) https://www.youtube.com/watch?v=87ptc3MVWLk

Joint Base Lewis McChord 1A Audit - (Pt. 2) https://www.youtube.com/watch?v=DnTeWoKtkEo

The ACLU has stated “Taking photographs of things that are plainly visible from public spaces is a constitutional right – and that includes federal buildings, transportation facilities, and police and other government officials carrying out their duties. Unfortunately, there is a widespread, continuing pattern of law enforcement officers ordering people to stop taking photographs from public places, and harassing, detaining and arresting those who fail to comply.” https://www.aclunc.org/our-work/your-rights/photographers-and-photography
Recommended Reading

Security & Counter-Surveillance - Information Against the Police State


A Practical Security Handbook for Activists and Campaigns (v 2.7)

Anonymous - Survival Guide for Citizens in a Revolution

Motherboard Guide to Not Getting Hacked

The Grugq - OPSEC: Because Jail is for wuftpdl (Youtube Video)
https://www.youtube.com/watch?v=9XaYdCdwiWU