This document is a translation into English of the original Japanese version. It was translated using machine translation (DeepL) and may contain inaccuracies. The documents linked to or accessible via QR codes may be in Japanese.

To Counter Espionage and Surveillance

From things you can do on your own to things you can do with others

JCA-NET jca.apc.org

Designed by macrovector / Freepik

Table of Contents

1. The Creation of Intelligence Agencies, Cyberwarfare, and the Rise of a Surveillance Society

1.1. Changes to Laws and Institutions

The Japanese government has been steadily moving forward with the creation of new legal frameworks and government organizations that enable the collection of our online communications data. The government's current goal is;

- to establish a system that allows for the widespread use of personal information held by the government and local authorities without the individual's consent
- to ensure that the government can access personal information held by the private sector by securing the cooperation of private telecommunications carriers and other entities

and other such measures.

The Constitution guarantees the right to privacy of communications and prohibits censorship, and there are various laws and systems in place to protect our fundamental human rights. Unfortunately, however, new laws and systems that undermine these rights have been introduced one after another.For example, during the 2026 session of the Diet, the National Intelligence Council/Intelligence Agency—aiming to become a spy agency on par with the U.S. CIA and NSA—was established. At the same time, a revision to the Act on the Protection of Personal Information was enacted, allowing for the collection and use of personal information without the individual's consent. Other measures that have been implemented include the Act on the Protection of Specified Secrets, which prioritizes national security; the security clearance system for background checks on workers; and the expanded use of the My Number system and My Number cards.Furthermore, from the spread of cashless payments via smartphones to the AI-equipped surveillance cameras now throughout cities, the ability to track people's daily activities has become significantly more sophisticated. Moreover, data centers currently under construction across Japan are accumulating vast amounts of personal information from around the world, and we cannot rule out the risk that this information may be used in the future as a tool for a highly surveillance-oriented society or for warfare.

1.2. Information Collection and Surveillance Are All Around Us

The government and private companies collect personal information from the communication infrastructure we use every day. Activities essential to daily life—such as email, social media, online shopping, web searches, weather and map services, and watching or streaming videos—also serve as means to track our movements. Therefore, it is crucial to reevaluate our daily online habits, take steps to prevent information from being collected, and make efforts to ensure we become neither victims nor perpetrators in a surveillance society.

1.3. Lack of Perceived Impact

A major problem is that we cannot truly grasp this reality because vast amounts of data are collected behind the scenes, beyond the reach of our five senses. Because we cannot feel it, it is extremely difficult to prevent or avoid the unintended collection of our information. It is also not easy to defend our privacy and individual rights by relying solely on our subjective perceptions.

The first thing we must do is make data collection visible. By making it visible, we can identify concrete measures to block unwanted data collection.

1.4. The Side Effects Last a Lifetime

Since individual pieces of collected information may seem trivial and not necessarily identifiable to a specific person, they may not be treated as important privacy data. However, when vast amounts of such seemingly trivial information are collected, it can be used to identify individuals or linked with critical privacy data, thereby serving as the foundation for monitoring our lives. Once information is collected, it is impossible to retrieve it. The side effects caused by collected personal information can last a lifetime.

1.5. About This Pamphlet

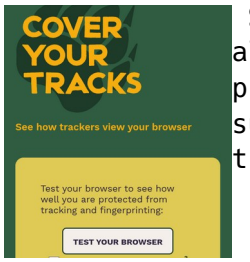
This pamphlet begins by introducing practical methods to visualize what kinds of data are being collected without our knowledge, slipping past our awareness. Building on that, it outlines the fundamental principles we—as citizens living in a surveillance society—should adopt to continue sharing information without feeling intimidated, including what precautions to take and what countermeasures are available.

This pamphlet introduces alternative tools that help avoid information theft and place greater emphasis on human rights and privacy. The selection criteria for the tools introduced here are as follows:

- The tools must be open-source or free software. As a general rule, we do not feature for-profit services that do not disclose their technical specifications.
- We introduce alternatives to services provided by companies that support war efforts.
- Smartphones and computers use a variety of operating systems. We introduce tools that can be used on virtually any device (with some exceptions).

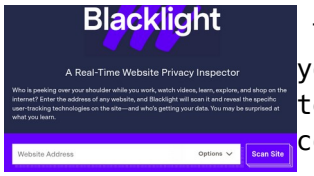
This pamphlet contains some technically challenging content, but feel free to skip over any parts you don't understand. You don't have to follow the pages in order—start with what you feel comfortable doing or what interests you most.

2. Understanding Data Collection



Suppose you use a browser to access a website. At that moment, although you may not realize it, the website collects various pieces of information about you. The amount of data is surprisingly vast. To see exactly what data is being tracked through your browser, visit the site below.

https://coveryourtracks.eff.org/



The Blacklights website scans the URL of the site you're visiting and reveals the user tracking technologies used on that site, as well as who is collecting your data.

https://themarkup.org/blacklight

If you regularly use Gmail or other Google services, Google's Privacy Policy is a must-read. It takes quite a bit of effort to read through it all the way to the end, but it explains just how much personal information Google collects.

https://policies.google.com/privacy?hl=ja

If, after reading this privacy policy, you determine that it is difficult to implement optimal privacy measures while using Google's services, we recommend switching to alternative tools such as those listed in this pamphlet.

When it comes to email, you can verify a great deal of information by viewing

the “email headers,” which are usually hidden. However, since header information is full of technical terms and can be difficult to understand, please refer to the following website: Japan Data Communications Association, “How to Check Email Header Information”

https://www.dekyo.or.jp/soudan/contents/ihan/header.html

Alternatively, please refer to the guidebook on the right: Toshikatsu Masui, *me-ru gijutu no kyokasho(in Japanese)*, Shoeisha.

3. What is being used as a means of information gathering and manipulation?

The following are the means used to collect our data.

- Communications via smartphones and computers (mobile payments, social media, email, web browsing, etc.)
- Personal data held by the government and local authorities (data linked to My Number, driver's licenses, criminal records, personal data obtained from private companies, etc.)
- Personal data held by financial institutions and medical institutions
- Surveillance cameras installed on city streets
- Devices known as the Internet of Things (IoT), such as Wi-Fi routers and smart electricity meters

Government intelligence agencies also use these channels for information gathering and manipulation.Intelligence agencies share information held by the government and acquire the legal and institutional authority to access private information as well. At the same time, they mobilize social media influencers and others to organize sophisticated information manipulation and incitement campaigns. Even in many countries that profess to be democracies—including the EU—intelligence gathering and information manipulation for national security purposes are generally treated as exceptions to the protection of human rights, such as the right to privacy.

As this makes clear, the smartphones and computers we use most frequently in our daily lives serve as the primary entry points for government information gathering and manipulation. That is precisely why it is crucial to block these entry points as much as possible.

4. What Can We Do?

When sending or receiving messages or logging into websites, we use a combination of an ID and a password to protect against identity theft and information theft. Passwords (or passphrases) are the most basic and essential requirement for safeguarding the confidentiality of our communications.

4.1. Review Your Password (Passphrase) Settings

Accounts and login IDs can potentially be discovered by third parties, and keeping them secret is not realistic. The only way to protect these accounts and IDs is with a password (passphrase). A passphrase refers to a combination of multiple words. In this pamphlet, the term “password” will be used to include passphrases as well.If a government intelligence agency or similar

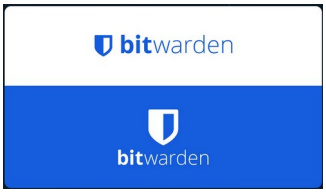
entity obtains a combination of your account (ID) and password, they can do anything—from reading your emails to impersonating you to stealing data such as your address book. Furthermore, you may be exposed to serious attacks, such as having malware planted on your device. Password management is an essential and critical matter. Please fully understand that even if you use strong encryption services, the encryption will be ineffective if you neglect to manage your passwords properly.

4.1.1. When setting a password, be sure to follow these rules

- Do not reuse the same password.
- Avoid using your name, date of birth, phone number, address, or easily guessable sequences like “1234” or “abcd,” as well as words found in a dictionary.
- Passwords must meet the above conditions and be at least 18 characters long.

4.1.2. What to Do If You Have Trouble Managing Passwords

It is nearly impossible to manage multiple passwords that meet the above criteria relying solely on your memory. By using reliable password management software, you can easily manage numerous complex passwords without having to reuse them. The following are some well-regarded options:

Password Management Software	Description
 Bitwarden https://bitwarden.com/ja-jp/	A detailed explanation is provided below. https://bitwarden.com/ja-jp/help/
 KeepassXC https://keepassxc.org/	A Japanese translation of the beginner's guide is available below. https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/keepassxc_gettingstarted/

4.1.3. Do not use fingerprint or facial recognition

Since entering passwords can be a hassle, you might be tempted to use facial or fingerprint recognition. However, we do not recommend these methods because there is a risk they could be used against your will. There is a real-life example where law enforcement obtained a court warrant and forcibly accessed a

smartphone using facial recognition:[1] .

4.1.4. An "analog" option: Get creative and write them down on paper

If you're going to reuse simple passwords anyway, it might be safer to discreetly hide a piece of paper with password hints in a place only you know about.Another option is to publicly post a version of your actual password that has been slightly modified according to a rule you've devised yourself. If you have only a few passwords, an analog method—such as carefully managing 18-character passwords without reusing them—is likely to provide higher security than struggling to learn how to use password management software that you're not comfortable with. We do not recommend using these methods in places where they might be seen by the general public.

4.2. Browser

4.2.1. What is the role of a browser?

The software required to access various web pages on the Internet is generally referred to as a “browser,” and there are many different types. Examples include Google Chrome, Microsoft Edge, Firefox, and Safari. Whether you're searching on Google, shopping on Amazon, reading the news on Yahoo, watching videos on YouTube, or checking your Gmail, you're doing all of these things using a browser. Sometimes, you may also access social media platforms like X or Instagram, or join Zoom meetings, through a browser. In this sense, browsers play the role of an indispensable, all-purpose tool for connecting to the internet and communicating. As mentioned earlier, since a great deal of data is provided through browsers in ways that aren't immediately apparent, it's very important to choose a browser that prioritizes privacy and incorporates mechanisms to block hidden trackers.

4.2.2. HTTP and HTTPS

Web URLs can start with either “http” or “https.” When you access an “http” site, there is a risk that all data transmitted over the connection—such as passwords and credit card numbers—could be intercepted by third parties. On the other hand, with “https,” the data transmitted over the connection is encrypted, significantly reducing the risk of interception. If you operate a website that currently uses “http,” please take the necessary steps to migrate it to “https” as soon as possible.

If you absolutely must access an HTTP site, please act as if your communication is being monitored by third parties at all times.

4.2.3. (Temporary Measures) Review your browser's “Settings” to ensure you are not inadvertently providing unnecessary data to others.

Open your browser's “Settings” screen. You can usually find the “Settings”

[1](Asahi) “Mandatory Smartphone Facial Recognition: A New Technique in Police Investigations—Concerns Over Going Too Far(in Japansese)” 2026/8/12_ https://digital.asahi.com/articles/ASV7Y34MQV7YPTIL014M.html

screen by clicking the hard-to-recognize icon—such as three horizontal lines or three dots—in the upper-right corner of the browser, which will display a menu from which you can select “Settings.”

1. Setting Change (Part 1): Switch from Google or Bing to a privacy-focused search engine, such as DuckDuckGo.

Since search behavior cannot be faked, search services like Google attempt to determine our interests based on what we search for. Switching to a privacy-focused search engine is the simplest way to counter this data collection. Find the “Search” section in your browser's “Settings” menu and change the “Default search engine” to one of the following:


DuckDuckGo https://duckduckgo.com/

ecosia https://www.ecosia.org/

Startpage https://www.startpage.com/

2. Setting Change (Part 2): Strengthen Tracking Protection.

Look for the section in the “Settings” screen where you can change privacy and security settings. Then, change the settings to be stricter than the default. For example, in Firefox,

- change “Enhanced Tracking Protection” from “Standard” to “Strict.”
- Set Firefox to delete cookies and site data when you close the browser.

3. Setting Change (Part 3): Add Extensions to Block Ads and Tracking.

Every browser has a built-in mechanism for adding features. These are called “extensions.” Click the settings icon (three horizontal lines or three dots) in the top-right corner of the browser and install various extensions from the “Extensions” section.

Among browser extensions, there are those that hide ads when you visit websites or block tracking (as described below). In the United States, there have been reports of the government obtaining data collected by commercial advertisements —which track user location and other information—and using it to monitor users.[2] As public-private partnerships are being established in Japan as well, the risks associated with user tracking through advertising are increasing.

To prevent such misuse, install the uBlock Origin and Privacy Badger

[2] https://www.404media.co/cbp-tapped-into-the-online-advertising-ecosystem-to-track-peoples-movements/

extensions in your browser. uBlock Origin is well-known for blocking ads, while Privacy Badger is renowned for blocking online tracking. In addition to these, installing the NoScript extension can further enhance protection against your computer being hijacked when you access the web.

How to Install

For Firefox-based browsers (Firefox, LibreWolf, Mullvad) , you can search for the names of the above extensions on the site below and install them.

https://addons.mozilla.org/ja/firefox/

Alternatively, you can find the extension by clicking the settings icon ⇒ “Extensions and Themes” and using the “Find Add-ons” search bar.

For Chrome-based browsers (Vivaldi), install the extension from the Google Chrome Web Store: .

https://chromewebstore.google.com/

However, due to Google's policies, uBlock Origin's full functionality is not available in Google Chrome. We recommend switching to a browser other than the Google Chrome family, as suggested below.

uBlock Origin “Quick Guide: Pop-up User Interface”

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/ublock-origin_quick-guide-popup-user-interface_jp/

Fight (EFF) Online Tracking Is Out of Control—Privacy Badger Helps Back

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_online-tracking-out-control-privacy-badger-can-help-you-fight-back_jp/

4.2.4. Switch to a browser that prioritizes privacy

We recommend switching from Google Chrome or Microsoft Edge to one of the browsers listed below. While they share similar core browser functionality, they offer features designed with privacy in mind. For computers, you can install them from the official website URLs listed below. For smartphones, install the app from Google Play for Android or the Apple Store for iPhone.

If you're unsure which one to choose, start by installing Firefox.

Firefox https://www.firefox.com/ja/

Vivaldi https://vivaldi.com/ja/download/

LibreWolf https://librewolf.net/

Mullvad https://mullvad.net/ja/browser

Tor https://www.torproject.org/

If you're a Windows or Mac user, or if you use an Android or iPhone smartphone, you can use the DuckDuckGo browser. (There is no version for Linux users.)

https://duckduckgo.com/

When switching from Chrome to Firefox, you can transfer your existing Chrome data (such as bookmarks and browsing history) to Firefox . Please refer to the instructions below.

Migrating from Chrome to Firefox

https://support.mozilla.org/ja/kb/switching-chrome-firefox

4.2.5. An "analog" option: The Library!!

We recommend using the library as a way to conduct research. The advantage of libraries is that you can get expert advice and search assistance from librarians. In open-shelf libraries, you can have the lucky experience of stumbling upon not only the materials you're looking for but also unexpected and interesting ones. The experience of reading an entire book is something you can't get online. Of course, there are also materials that exist only in print from a time before the internet even existed. Let's remember that libraries are treasure troves of information. An increasing number of materials from the National Diet Library have been digitized and are now accessible online. https://www.ndl.go.jp/

4.3. Reviewing Smartphone Security

4.3.1. Require a password for access

While it's convenient to be able to use your smartphone just by touching the screen, this also means anyone can use it. Keeping the risk of theft or loss in mind, set your device so that a password is required to use it.

4.3.2. Change the privacy and security settings in your smartphone's “Settings” to stricter settings.

- Turn off location services. Turn them on only when absolutely necessary.
- Restrict which apps can access your contacts.
- Turn off the camera and microphone when not in use. Cover the camera lens.
- Switch to a privacy-focused browser.
- Delete apps you don't use or don't recognize.

Smartphone settings are often complex and confusing, which can be disorienting. Please refer to the following for guidance.

(EFF) How to Configure Privacy and Security Settings on Android

_

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_android-how-to-get-to-know-android-privacy-and-security-settings/

(EFF) How to Set Up Privacy and Security on an iPhone

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/effiphone-how-to-get-to-know-iphone-privacy-and-security-settings_jp/

4.4. Understand the Risks of Social Media

4.4.1. Avoid Using In-App Browsers

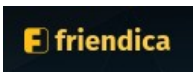
If a link is included in a social media message, the social media platform's built-in browser will be used to access the website. Even if you set strict privacy settings on your default browser, these settings do not apply to the social media platform's browser, which can lead to the unintended theft of personal information. Even if it's a hassle, please copy the link from the social media platform and open it in your default browser.

4.4.2. The Algorithm Behind Viral Sharing

Viral sharing on social media is a crucial means of publicity for civic and social movements. However, please remember that this sharing depends on social media algorithms and is driven by for-profit services. If you hand out flyers on the street, most people won't take them. This is the true power of viral sharing.

It should be noted that not all social media platforms are operated by algorithms designed for profit. For example, here are a few examples of non-profit, ad-free social media platforms that have fewer arbitrary algorithms and less hate speech. These platforms are interconnected. For instance, you can read or follow posts made on Mastodon via Friendica.

Mastodon https://joinmastodon.org/ja An alternative to X.



Friendica https://friendi.ca/ Allows for long-form posts.

Pixelfed https://pixelfed.org/ An alternative to Instagram.

PeerTube https://joinpeertube.org/ An alternative to YouTube.

4.4.3. Followers as “Hostages”

Even if you're fed up with ads, hate speech, and misinformation, it's not easy to break away from social media platforms with a large following. Mainstream social media platforms hold your followers hostage to prevent you from switching to other platforms. However, start by sharing content on alternative platforms like the ones listed above, and consider transitioning to a new social media platform as part of a long-term plan.

4.4.4. Avoid using services from companies complicit in genocide and hate speech as much as possible

Major social media platforms like X, Facebook, and Instagram have become tools for propaganda that incites war. Furthermore, during the genocide in Gaza, there have been frequent instances of censorship and measures to suppress the spread of posts by Palestinian residents within Israel. Major Big Tech companies like Google, Amazon, and Microsoft have provided the infrastructure—such as airstrikes—that has enabled genocide. Precisely because these companies provide services essential to our daily lives, switching to alternative services whenever possible is an important way to make our stance known.

4.5. VPN

When you connect to the internet to use services, your internet service provider (ISP) assigns you an IP address. ISPs can record everything, including which websites you visit, and this can be used to track your online activities. A VPN (Virtual Private Network) is a service that hides this IP address from your ISP. Here are two examples.

ProtonVPN https://protonvpn.com/ja

MullvadVPN https://mullvad.net/ja/vpn

MullvadVPN is paid-only. It costs 5 euros per month. You can pay monthly, and since there's no automatic renewal, your subscription will be canceled the

following month if you don't pay. It's worth giving it a try. ProtonVPN offers a free version, but the network can sometimes be congested.

While a VPN can hide your access information from your internet service provider, the VPN provider itself can track your destination. It's essential to choose a trustworthy provider that prioritizes user privacy above all else.

Using a VPN is generally very straightforward. Simply install the app, and you're ready to go. Even just setting your access point to a location different from where you live can help hide your location.

4.5.1. An "analog" option: Surprisingly Secure Snail Mail Delivery

Even today, when digitization is the prevailing trend in society, sending passwords via sealed mail is sometimes used—for example, when requesting a password reset from your service provider. It's also common for government agencies and financial institutions to send important documents by snail mail. Sending private information via sealed mail still offers a level of confidentiality that online communication lacks. Although it takes time and costs money, keep in mind that postal mail remains a viable option when necessary. Perhaps even carrier pigeons might be a good choice.

4.6. Maps: From Google Maps to OpenStreetMap

The most common method is probably to turn on your smartphone's GPS and navigate to your destination while viewing the route on Google Maps. However, I recommend using OpenStreetMap, an excellent open-source map service. It's feature-rich and even allows you to edit the maps yourself. It might take a little time to get used to, but considering that you won't be tracked by Google, the effort will be worth it.

Below is a beginner's guide on how to use it.

OpenStreetMap

https://learnosm.org/ja/beginner/

4.6.1. An Analog Option: Paper Maps and Compasses

We shouldn't sacrifice the skill of using paper maps and a compass—a skill humanity has mastered over a long period—simply because of the widespread use of digital devices. Try discovering the unique benefits that paper maps and compasses offer, which digital tools lack. I also highly recommend reading M.R. O'Connor's *Wayfinding: The Science and Mystery of How Human s Navigate the World*.

4.7. Encryption Services

4.7.1. Encrypted Email Services: Proton and Tuta

The Japanese government is establishing a system to compel telecommunications providers to cooperate and hand over communication data. While emails are encrypted over communication lines, making them difficult to intercept, the data is almost always stored unencrypted on the providers' servers. There is a

possibility that your telecommunications provider may prioritize cooperation with the government over users' rights to privacy and the confidentiality of communications.

One way to prevent telecommunications providers from providing communication data to the government is to use an encrypted email service. Neither the government nor the telecommunications provider itself can access the data unless it is decrypted, and they are unable to decrypt it.

Proton Mail

Proton: Based in Switzerland. In addition to email, it offers various encryption services such as calendars, cloud services, and VPNs (see section 4.5 above). https://proton.me/

tuta

tuta: Based in Germany. In addition to email, it offers encrypted calendar services. https://tuta.com/

Encrypted email also has its disadvantages. Unless both parties use the same service, they cannot communicate securely in both directions (end-to-end encryption). If the recipient uses an unencrypted email service like Gmail, emails sent from Proton or Tuta will be stored in the recipient's inbox in unencrypted form. However, emails from the recipient will be encrypted and stored in your Proton or Tuta inbox. The fact that the emails you receive from the other party are protected is a significant benefit in itself. Furthermore, with Proton, you can exchange encrypted emails with external parties by using PGP encryption or password protection. Tuta also offers password protection.
How to Use PGP with Proton Mail

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/proton-mail_how-to-use-pgp/

How to Send Encrypted Emails for Free with Tuta Mail

https://tuta.com/ja/blog/email-encryption-guide-how-send-encrypted-email

4.7.2. Encrypted Messaging Service: Signal

In the case of LINE, which has the largest user base in Japan, there were approximately 7,000 requests for user information disclosure from law enforcement agencies and other entities in the second half of 2025, and there has been a sharp increase in information disclosures resulting from investigative inquiries not based on court warrants.[3] Signal offers services nearly identical to LINE, such as group chats, video conferencing, and phone calls, and its usage is similar; it is the most highly regarded service for message encryption.

Signal

https://signal.org/ja/

[3] https://www.lycorp.co.jp/ja/privacy-security/privacy/transparency/reports/2025h2/

4.7.3. Cloud Data Encryption: CryptPad

CryptPad allows you to create documents, work on spreadsheets, manage schedules, and perform various other tasks while keeping your data encrypted and secure. You can use CryptPad to handle many of the same tasks you would perform in Google Docs. Collaborative work is also supported. Since CryptPad is open source, you can install it on your own server to host the service, which is why there are hosting sites all over the world.

https://cryptpad.fr/index.html Hosted by the development team.

https://cryptpad.org/instances/: A list of publicly available CryptPad instances.

4.7.4. Is encryption impossible without using these services?

Not at all. There are various methods of encryption. There is software available that allows you to encrypt documents on your own computer. Alternatively, you can encrypt your entire computer's hard drive. Encryption mechanisms also vary. If you'd like to learn more about encryption, please read the booklet below.

Glencora Boradale, *Defend Dissent: Digital Supression and Cryptgraphic Defense of Sovcial Movements*
https://open.oregonstate.education/defenddissent/

For those without technical knowledge, using encryption services like the ones introduced above is the quickest way to benefit from encryption.

4.7.5. Can this kind of encryption really counter government spying?

Yes, it can. Cryptographic technology is built purely on mathematical theory. Trustworthy cryptographic technologies make their technical specifications public so that anyone can verify them. If you come across an encryption service that tries to sell itself with a slogan like, “Our encryption technology is a bussiness secret, so we don't disclose it,” you should absolutely avoid using it. Services that cannot be verified by third parties lack credibility. The services introduced above—such as Proton, Tuta, and CryptPad—are all open-source and publish their technical specifications.

4.7.6. When it comes to encryption, the most important thing to watch out for is, of course, your password!

When encrypting data or restoring (decrypting) encrypted data, you'll need to enter a password. Strictly adhering to password policies and managing them properly is an essential prerequisite. No matter how strong the encryption is, it's completely ineffective if you use a weak password.

4.7.7. If encryption is so effective against government espionage, doese that mean government espionage isn't really that much of a threat?

As mentioned at the beginning of this pamphlet, our information is being stolen through mechanisms we are unaware of. The threat posed by this is extremely serious precisely because we are unaware of it. It is important to understand this and take measures such as encryption to the greatest extent possible. Even if vast amounts of encrypted data are collected, it cannot be decrypted and is therefore useless. For this reason, the Japanese government, along with the United States, Australia, and others, is even attempting to regulate our use of encryption itself. Citing various reasons—such as child pornography, terrorism, and measures against organized crimes—they are plotting to expand their legal authority by legally banning encryption services or weakening the strength of available encryption. Such efforts are already taking concrete form in the EU as well.

Encryption is the very essence of our right to privacy. We must resolutely oppose any efforts to criminalize the use of encryption.

4.8. Anonymity

Voting is anonymous, and shopping with cash is also anonymous. Whistleblower systems should also be protected by the right to anonymity. Anonymity is fundamental when participating in demonstrations and rallies. It is precisely because of anonymity that we are given the courage to denounce those in power or voice dissent against the prevailing opinion.

However, we now live in an era where the right to anonymity can be infringed upon by the collection of vast amounts of data and the piecing together of trivial fragments of information like a jigsaw puzzle. Given the history of intelligence agencies monitoring those who dissent against the government, it is crucial to take measures to act as anonymously as possible. Email, in particular, makes it easy to identify the sender based on their account. Services like DuckDuckGo offer email anonymization to address this vulnerability. By using an anonymization service for email addresses when subscribing to newsletters from government agencies or registering on shopping sites, you can ensure that your real email address remains unknown to the recipient.

(DuckDuckGo Mail) Protect your inbox: The beta version of DuckDuckGo Email Protection ( ) is now available to all users!

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/duckduckgo-mail_protect-your-inbox-with-duckduckgo-email-protection_jp/

4.8.1. An Analog Alternative: Pay with Cash

Whether you use a mobile wallet or a credit card, any payment method other than cash will inevitably leave a record of your transaction data. It is extremely difficult to achieve a level of privacy protection in the digital realm that matches the anonymity of cash. If you value your anonymity, it's important to make it a habit to pay with cash whenever possible.

4.8.2. An Analog Alternative: Stop Using the My Number Card and My Number Health Insurance Card

The My Number Card serves as a means to track the cardholder's usage patterns. The My Number Health Insurance Card also serves as a means to collect medical information beyond the scope of medical treatment. How the collected information will be used in the future depends on laws and regulations, but there is a clear trend toward its expanded use. Furthermore, while it is convenient to handle resident services without visiting city hall, visiting government offices and understanding their actual operations is a fundamental aspect of democracy. Completing procedures at city hall is also an important exercise of your rights.Let's return our My Number Cards and use eligibility verification certificates and medication records instead of the My Number health insurance card. For more details, please visit the "We Don't Need a Common Number (My Number) Network Blog" at https://www.jca.apc.org/activist/.

4.9. Online meeting system: Jitsi-meet

Jitsi Meet is an online conferencing system that serves as an alternative to Zoom. It works well for meetings of about 20 to 30 people, and can accommodate more than 50 participants as long as everyone except the speaker keeps their cameras off. Unlike Zoom, the servers hosting the meeting rooms are independent, and they are operated by various entities. It is important to choose a trustworthy server. We recommend the following servers.

Developer Site
https://meet.jit.si/

JCA-NET https://jitsi-01.jca.apc.org/

Framatalk https://authent.framatalk.org/

For instructions on how to use Jitsi Meet, please refer to the JCA-NET manual below.
https://jca.apc.org/jca-net サービスについて/オンライン会議システム jitsi-meet マニュアル/

4.10. Switching Mailing Lists from Google Groups to Frama Groups

While Google Groups has become the standard for mailing list services, there are excellent alternatives that prioritize privacy. For example, Frama Groups is a service provided by Framasoft, a France-based organization that advocates for moving away from Google.

Framagroupeshttps://framagroupes.org/abc/en/

5. Refuse to Cooperate with War; Fight Against Government-Private Sector Information Gathering

5.1. State espionage is also part of war

Israel's war in Gaza is also a new form of cyberwarfare. It has become clear that major IT companies—which are part of our daily lives and provide services that have become essential online—are deeply complicit in Israel's genocide in Gaza.

For example, companies like Google, Amazon, and Microsoft can be considered war-crimes enterprises complicit in genocide, as they provide the information and systems that enable the airstrikes and drone attacks responsible for the killing of numerous people in Gaza.

Meanwhile, social media companies such as X, Facebook, and Instagram collect user data and use it for surveillance and repression. While censoring the voices of the Palestinian people and suppressing the spread of information, they have maintained policies that tacitly condone posts inciting Israel's genocide and hate speech directed at the Palestinian people.

The involvement of information and communications technology companies in war is not limited to U.S. multinational corporations. For example, Japan's Rakuten announced a partnership with the German arms manufacturer "Helsing"[4], prompting concerned companies to boycott opening stores on Rakuten's platform. Continuing to use the services of companies complicit in war effectively amounts to tacit approval of their crimes—including complicity in government-sponsored warfare and espionage, as well as human rights violations. Refusing to use the services of companies complicit in war and the surveillance state is something you can start doing today.

5.2. Even if boycotting Windows is difficult, there are still things you can do

Unlike Google and Amazon, Microsoft provides Windows, the operating system (OS) for personal computers, so boycotting Windows itself may be difficult. However, it is not impossible to stop using Microsoft's "Office Suite"—standard software like Word, Excel, and PowerPoint that is commonly used in the workplace—and switch to LibreOffice, for example.

https://ja.libreoffice.org/

Another option is to switch to CryptPad (see "Using an Encryption Service" above).

6. Building a Community Is Most Important—Let's Start a Discussion

With the establishment of government intelligence agencies—such as the National Intelligence Council and the National Intelligence Agency—plans are in

[4] https://jp.reuters.com/economy/ZKGNP2C7YNI53EI7HUU7FZGFBE-2026-08-17/

place to strengthen public-private partnerships and establish a comprehensive and powerful intelligence-gathering system. In light of this unprecedented situation, it is crucial for those involved in civic movements and similar initiatives to first discuss the situation with their peers, work together on actions they can take, and change the culture of activism surrounding the communication environment.

To that end, it is essential to develop a shared understanding of how government intelligence agencies—working in collaboration with the private sector and with foreign governments such as the United States—intend to collect our information.While setting up security measures for smartphones and computers—including configuring passwords—can be a hassle, it is extremely important. Please take on this challenging task by discussing these matters with one another. Reevaluate the services you use and, wherever possible, switch to options that prioritize privacy and are less susceptible to data theft. Furthermore, it is crucial to support those among you who are not tech-savvy.

7. Frequently Asked Questions

7.1. The government's power is so immense that it seems useless to do anything at all.

It's not a waste of effort. There are many things the government cannot do within the online environment. For example, the Internet cables and radio waves that span the globe are now almost entirely encrypted, making it impossible for the government to monitor their contents. As a result, the government has no choice but to rely on cooperation from private telecommunications providers to obtain data. Encrypting data on servers, smartphones, and computers is an effective countermeasure against the government's information gathering efforts.

7.2. What is a defensive strategy that works for everyone—one that, by doing just this, ensures you’ re fully protected?

One thing you absolutely must do is manage your passwords properly. This is a precaution everyone should take. However, this alone does not guarantee complete protection. First, you need to assess what poses the greatest risk to you personally. Then, you should research what defensive measures you can take. Since the priority of these risks varies depending on each person's individual circumstances, there is no one-size-fits-all solution.

7.3. Will taking care of minor details like passwords and privacy really have any effect against the government's vast surveillance capabilities?

It certainly does. By taking these steps, you will definitely reduce the amount of information collected about you, and as a result, the amount of information collected about the people connected to you will also decrease. If you go to the polls to vote, even though a single vote can't possibly change the world, you must have your own reason for doing so. That same reasoning applies here. If you've ever participated in a demonstration with dozens or

hundreds of people, you probably have your own reasons for taking action—even though you know a small demonstration like that is unlikely to change the government's stance. That same reasoning applies here as well. And above all, please remember that each of us lives within a network of social connections, and protecting your own information also helps protect the information of the people connected to you.

7.4. I don't know much about the internet or computers, so I'm hesitant to get involved.

People’s movements and various social movements have a proven track record of tackling highly complex technical issues head-on. For example, many people have opposed nuclear power plants and nuclear weapons without being experts in nuclear physics or related fields. Even on issues like the harms of pesticides and chemical fertilizers or the adverse effects of pharmaceuticals—where the detailed mechanisms are difficult to grasp without specialized knowledge—people have boldly taken on these challenges and fought for change.

Even without understanding the details of specialized knowledge or technical mechanisms, it is possible to grasp the essence of a problem and fight with a sense of urgency. The same applies to the cyber space. Even if we “don't understand” something, we can still recognize that it is a serious problem we must confront.

7.5. You may not have anyone around you who is knowledgeable about the internet or computers. There may be many things you don't fully understand yourself. What should you do?

If you or your fellow activists in a people’s movement are facing such issues, please feel free to consult with JCA-NET.

JCA-NET supports your efforts regarding internet and computer security. First, let's have a casual get-together—even if it's just two or three people. A JCA-NET member will join you to share your questions and discuss possible solutions.

You can download the PDF version of this pamphlet from the link below. We will also gradually post additional information and explanations on this page that could not be included in the pamphlet: . Please make use of this resource.

https://jca.apc.org/jca-netの取り組み/スパイ・To Monitor and Resist—What One Person Can Do/

Author: JCA-NET ¦ Published: September 20, 2026
Free. If you find this helpful, please consider making a donation. This pamphlet was produced using JCA-NET membership dues and donations from the public.
Postal Transfer Account: JCA-NET (J-C-A-NET)
Account Number: 00190-3-417584, Japan Post Bank Branch 019, Account 417584
*Please write “Donation” in the message field.

JCA-NET Contact: , Toshimaru 070-5553-5495 toshi@jca.apc.org

https://jca.apc.org