GlobalResearch
Center for Research on Globalization

What Does the US Government Know About You?

By Dennis Anon
Global Research, August 17, 2018
Privacy.net 17 February 2018

Region: USA
Theme: Intelligence

Note to readers: please click the share buttons above

How much does the US government know about you? It's not a question easily answered. The US government operates the largest and most advanced spying, surveillance, and data collection programs on the planet. It's made up of multiple law enforcement and intelligence agencies, some of which operate in secret. The federal government, of course, consists more than two dozen major agencies that perform regular record keeping for operational purposes, such as the Internal Revenue Service, Department of Housing and Urban Development, and Social Security Administration.

Aside from official government entities, third parties often comply with government requests for information. These include big tech companies like Google, Apple, Microsoft, and Facebook, all of which were shown by Edward Snowden to have cooperated with the NSA's spying efforts. And while we're thinking about Edward Snowden, recall that he was a private contractor at the NSA at the time and not a government employee. Contractors and private companies can collect information on behalf of the US government as well.

The amount and accuracy of information that the government varies from one person to the next. Someone who spends a lot of time online, sharing on social media, creating accounts at different services, and/or communicating with friends and relatives overseas will leave a much more clear trail of data than someone who shuns Facebook and takes proactive steps to protect their privacy. Government employees must undergo rigorous background checks, while someone getting paid under the table at a local restaurant can fly under the radar.

Attempting to cover all the information that the US government knows about any one person quickly becomes overwhelming and full of caveats. With all of this in mind, it's clear we need to narrow down our parameters. To that end, we'll create three typical archetypes–Alice, Bob, and Chris–who fit the following profiles:

Alice is:

- A naturalized citizen (immigrant)
- Middle aged
- A private sector employee
- A frequent online shopper
- A tenant in a rented apartment
- A college graduate

Bob is:

- A US citizen from birth
- Elderly
- Retired from the public sector
- Not very computer-literate and doesn't spend much time online
- A homeowner

Chris is:

- A minor
- A public school student
- Active on social media
- Applying for college
- Doesn't have a job

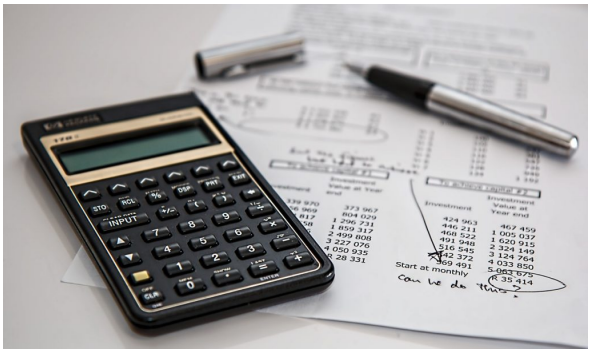
To narrow our scope a bit further, let's assume none of these three people has a criminal record. They are all US citizens, either from birth or naturalized. None of them have served in the military or law enforcement. They do not collect welfare such as unemployment checks, food stamps, worker's compensation, or disability benefits. Finally, we'll only cover information that the government can legally collect without a court order.

We'll categorize the types of information based on, in broad strokes, who originally collects it:

- Non-law enforcement government agencies – Mostly routine information that the government needs to operate and is not collected for intelligence or law enforcement purposes
- Intelligence and law enforcement agencies – Information swept up in government spying and surveillance programs
- Non-government companies – Private companies, credit bureaus, public utilities, and other entities not operated by the government but that cooperate with government requests for information

Info collected by non-intelligence agencies

Some information is required for the US government to effectively operate and serve the public. This includes information that's used collect taxes, dole out welfare, deliver mail, draw boundaries for congressional and school districts, and assess social and economic trends and make policy decisions.



While we say this information is "routine", once it's all combined, one could actually formulate a fairly intimate depiction of a person's life. The US government likely knows the

following about all three of our hypothetical characters:

- Name
- Social security number
- Permanent address and/or place of usual residence
- Age, birth date
- Place of birth
- Prior place of residence and duration of residence
- Ethnicity
- Marital status
- Household composition (family members and how they're all related)

This information can be collected through various means, including tax forms, the postal service, and census data.

The decennial census in particular gathers a large amount of personal information. Individual information is kept private for 72 years; the latest census data available to the public is from 1940.

You might presume that intelligence and law enforcement agencies can access Census records whenever they want, but think again. The US Census Bureau is bound by Title 13 of the United States Code, guaranteeing confidentiality. The FBI and other government entities do not have the legal right to access this information. So the US government technically knows a lot about you through the Census and IRS, but, on paper, that information is locked away and only used in aggregate.

The IRS is a bit different. IRS.gov's page on disclosure laws notes, "pursuant to court order, return information may be shared with law enforcement agencies for investigation and prosecution of non-tax criminal laws." That means all the information in your tax return can be used by the FBI and other law enforcement agencies with a court order. The IRS actually uses some of the same surveillance techniques as national intelligence agencies, including deployment of Stingrays to spy on cell phones.

Chris doesn't have an income yet and thus doesn't need to file his own taxes, but he is about to apply to college and thus will fill out a FAFSA to apply for federal student aid. He's also a public school student, so it's reasonable to assume the government knows the following about him:

- Education level
- What classes he takes
- Where he goes to school
- Parents' income from their jobs and investments
- Parents' employment status

Alice holds down a full-time job and files taxes every year. She also participates in the census as required by law. It's reasonable to assume the US government would know the following information about her:

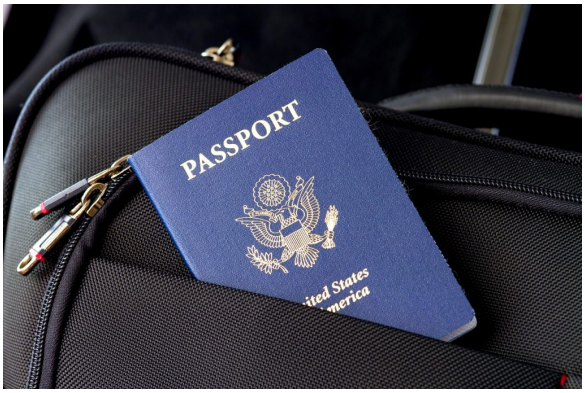
- Employment status
- Occupation and industry
- Income

- Place of work
- Education level
- Student loan payment status

Bob is retired and own his own home. He earns a modest pension and collects social security. Medicare pays for the majority of his medical expenses. He's also a bit of a philanthropist who regularly donates to charity. We can assume the government collects the following information about him in a given year:

- Income
- Current medicare and social security benefits, and estimate of future benefits
- Employment status
- Donations claimed on tax forms
- Education level
- Previous occupation and industry
- Medical history, medications
- Doctor(s) and hospital visits
- Property tax and valuation info, including:
    - Value of home and land
    - How the property is used
    - Location
    - Size
    - Improvements and problems
    - Easements
    - Type of access

While we're on the topic of social security, note that a regulation that required the SSA to to disclose information about certain people with mental illness to the national gun background check system. That regulation was nixed by President Trump in February 2017.



All three fictional characters could conceivably have a driver's license or passport. Driver's licenses are administered at the state level, but the data about drivers is presumably accessible by the federal government. These types of official photo IDs contain information like

- Name
- Home address
- Birth date
- Photo
- Sex

- Height
- Weight
- Eye color
- Signature

And don't forget: a driver's license means a driver's record as well, including a record of any past infractions. Bob and Alice own their own vehicles, which are registered with the following information:

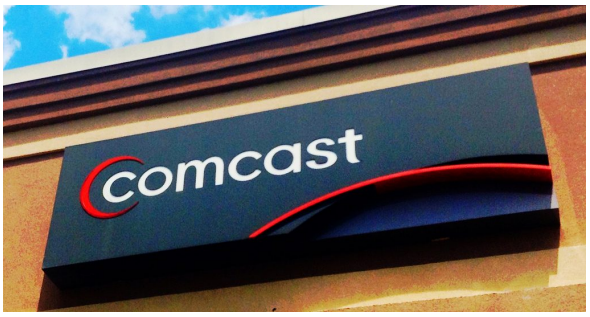
- Make
- Model
- Year
- Previous owners
- License plate number

Government-accessible info collected by private companies

In this section, we'll look at information collected by private entities, some backed by the government and others wholly private. These include internet service providers (ISPs), internet companies, utility companies and credit bureaus.

Info provided by ISPs and internet companies

The FBI and NSA perform their fair share of online surveillance, to be sure. But in many cases they might not be allowed to monitor who they want, when they want due to laws and regulations, particularly those about spying on US citizens. In many cases, however, intelligence and law enforcement agencies don't even have to conduct their own surveillance. It's much easier and more efficient to simply use data that private companies already have.



The FBI might ask for information regarding a particular redditor, like Chris, such as the IP address from which they access the site. The NSA might ask for the account names of everyone who typed in a particular search term in a certain period of time, e.g. Bob searching for information about his pain medication. The ATF could ask Amazon to set up an alert every time a customer purchases a specific book, such as if Alice buys a book about Islam. And the DEA could request your ISP hand over the browsing history of suspected drug dealers.

Internet companies earn revenue from the data they collect, so for many of them, more is better. How much they share with law enforcement without a court order depends on the company itself. Check the privacy policy and terms of service of your ISP or a website to see

what types of information they collect, with whom they share it, and under what circumstances. Most major companies now state that they don't hand over customer information without a court order. But when those court orders do come in, they often come paired with a gag order. Some guarantee no such protection and will cooperate with law enforcement, court order or no.

The information that websites and ISPs collect varies depending on the company and what you do online, but here's a list of possibilities:

- Browsing history
- Search queries
- Device name and unique ID
- IP address and location
- Videos watched, songs listened to
- Purchases
- Downloads
- Social media posts

In 2017, Congress repealed an Obama-era FCC rule that prevented ISPs from sharing browsing data with third parties like advertisers. With that rule out of the way, ISPs that control your access to the internet are expected to start gathering more data than ever on their users. If you don't want to be tracked by your ISP, we recommend signing up for a reputable VPN.

Library records and ebooks

48 states in the US have laws that protect library records from snoopers, and two have legal directives that serve a similar purpose. To access a person's library records, a court order is usually necessary.

That's more protection than you'll find on Amazon when buying an ebook. Amazon and other ebook sellers usually have privacy policies stating they also only hand over reader's private information with a court order, but there's technically no law barring them from doing so. Furthermore, Amazon can keep much better track of what you're reading and how you read on its Kindle devices and companion apps. Amazon can not only see what you read, but what page you're on, when you read, highlighted passages, and any notes you've scribbled into the ereader.

Only four states have laws about protecting e-reader data in libraries, so you're best checking out a physical book from your local library for maximum privacy.

Credit reporting agencies

All three of our hypothetical characters have credit reports maintained by one of the three major US credit bureaus: Experian, Equifax, and Transunion. Creditors and government agencies can access your credit report for background checks and other purposes. Credit reporting agencies are overseen by the Federal Trade Commission (FTC).

A credit report contains the following information:

- Name
- Address

- Social Security number
- Date of birth
- Trade lines (credit accounts)
    - Bank and credit cards
    - Auto loans
    - Mortgages
    - Date you opened each account
    - Credit limit or loan amount
    - Account balance
    - Payment history
- Credit inquiries
    - A list of everyone who accessed your credit report in the last two years, both voluntary and involuntary. The latter occurs when lender order your report to send pre-approved credit offers
- Public records and collections – Information on the public record aggregated from courts and collection agencies, including:
    - Overdue debt
    - Bankruptcies
    - Foreclosures
    - Suits
    - Wage garnishment
    - Liens

Of course, a hard lesson about keeping all of this information with just three companies was learned the hard way when Equifax was breached in 2017, leaking Social Security numbers and other details of more than 145 million Americans.

Other financial info

Most targeted surveillance on finances requires a court order, but that's not always the case. Human Rights Watch explains:

"In investigations related to international terrorism or espionage, the FBI can also demand bank account statements and credit card histories using a national security letter, which doesn't require a judge's approval – and which often comes served with a gag order."

For most of us, however, the government probably knows about accounts opened in your name, but not necessarily their contents or spending records.

If you invest in the stock market, then your investments are tracked by the Securities Exchange Commission and other official oversight bodies. Each state has its own blue sky law, which requires:

- Registration of all securities offerings and sales
- Stockbrokers
- Brokerage firms

The laws are less clear when it comes to cryptocurrencies like bitcoin. In late 2017, the IRS ordered the country's largest cryptocurrency exchange, Coinbase, to hand over information about all customers who made a transaction worth $20,000 or more between 2013 and 2015. That information includes:

- Names
- Birth dates
- Addresses
- Tax IDs
- Transaction logs
- Account invoices

Bitcoin and other cryptocurrencies are often thought of as anonymous, but if you have an account with a major exchange, then that exchange most likely requires such identifying information—not to mention a credit card or bank account—to purchase cryptocurrencies with fiat currency. In addition to the blockchain, which tracks transactions of all transactions on a cryptocurrency's network, following the paper trail is a simple matter.

Public utilities

Public utility companies, excluding telecommunications, require a minimum amount of information in order to deliver their services. Water, gas, and electricity companies can be private or public, but all companies classified as utilities undergo heavy government regulation because they are allowed to operate regional monopolies on the condition they serve the public. Utility companies know more about a household as a whole rather than specific people. The information they collect normally consists of:

- Name
- Address
- Telephone number
- Payment information (bank account and/or credit card number)
- Technical information about equipment on the residence necessary to deliver a service

The adoption of a smart grid that began during the Obama administration aim to allow consumers to use energy resources more efficiently. In particular, the rollout of smart meters allow property owners to better monitor and control their consumption of electricity and gas. However, this also raises concerns about the flow of detailed information not only between customers and energy providers, but also between tenants and their landlords.

A public utility company that installs a smart meter at your household could, even without detailed knowledge of the appliances you own, determine with reasonable certainty when you cook, shower, sleep, and leave the house,among other activities. According to a 2009 report published by the Colorado Public Utilities Commission stated the following:

"A remarkable number of electric appliances can be identified by their load signatures, and with impressive accuracy. Researchers have all but mastered identification of the larger common household appliances such as water heaters, well pumps, furnace blowers, refrigerators, and air conditioners, with recognition accuracies approaching perfection. Ongoing work focuses now on the myriad smaller electric devices around the home such as personal computers, laser printers, and [different types of] light bulbs."

The software algorithms and the smart meter hardware itself has likely gotten more advanced since then, so you can expect a commensurate increase in accuracy. In response to these concerns, a handful of states passed laws restricting how smart meter data can be used and by whom. These include California, New York, Ohio, and Colorado.

Info collected by law enforcement and intelligence agencies

Mass surveillance and metadata

In 2013, Edward Snowden shocked the world when he revealed a series of mass surveillance programs used to intercept communications of both Americans and non-Americans. The NSA and FBI argue that they do not record the contents of phone calls or emails without a court order and merely collected metadata about those calls.

The NSA, where Snowden worked as a contractor, collected data on millions of people's phone records from AT&T, Sprint, and Verizon. Phone call metadata includes:

- Phone number of both parties making and receiving the call
- How long the call lasted
- When the call was made

Snowden said the NSA secretly gained direct access to servers at Microsoft, Google, Facebook, and Yahoo, among other companies that participated in the PRISM program. Those companies denied the allegations outright, saying they only hand over information on a case-by-case basis with a court order, and not in bulk.

However, *The Guardian* reported in 2013 that the Bush and Obama administrations collected email metadata on any communication between non-US citizens or communications in which at least one party is outside of the US, even if they are an American citizen. The email metadata does not include the contents of emails, which, like phone calls, would require a court order. Email metadata includes:

- The email addresses of the sender and receiver
- A timestamp of when the email was sent
- An IP address used by people sending emails from inside the US
- Location based on the IP address

In 2012, the Department of Homeland security revealed in a lawsuit that it monitored social networks like Facebook and Twitter by running searches for keywords for at least a year and a half. The information swept up in the surveillance includes the contents of social media posts and comments. Chris' Facebook and Twitter posts could be swept up in such surveillance.

In short, the US government can legally obtain metadata about calls, messages, and emails, but not their actual contents. For that, a court order is necessary, although the person being investigated probably won't be notified in such an event.

Most of these programs were conducted under the Foreign Intelligence Surveillance Act (FISA) and/or the Patriot Act. Those laws are officially restricted to spying on non-US citizens, but many Americans' communications get swept up by bulk interception programs. Alice, a naturalized US citizen who has family in another country, would likely have her communications with them closely monitored by US intelligence agencies.

Spying on the contents of electronic communication typically requires a court order. Government agencies can and do collect metadata about emails, text messages, and phone calls, but not their actual content. The FBI or NSA can record the sender and receiver, time sent, call duration, and location of the correspondents without a warrant, but they'll need a court order to actually listen in or read your messages.

Location

A home and work address is far from the only way the government can track someone's location. Many of us now have at least one GPS-enabled device within at all times, likely a phone or vehicle with navigation capabilities. But GPS is a navigation system owned by the US government and operated by the US Air Force.

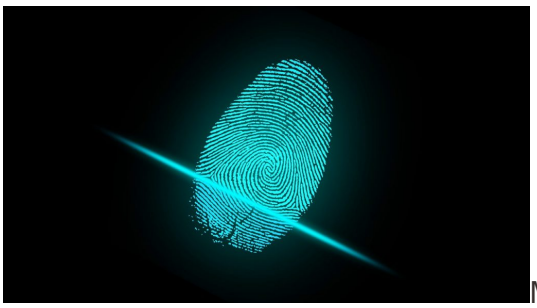
The law hasn't kept up and isn't entirely clear on whether law enforcement can use GPS data to track someone without a court order. A 2012 Supreme Court ruling states that law enforcement cannot place a GPS tracker on a suspect's vehicle without a warrant. However, that ruling doesn't take into account cars and smartphones with GPS already built in. We can assume that the government can hone in and record someone's movements using a GPS signal that they voluntarily broadcast into public airspace.

Even if Chris turns the GPS on his phone off, his approximate location can still be tracked by analyzing nearby wifi networks and cell towers that his phone pings whenever its in range. All internet-connected devices also have a unique IP address that's assigned in accordance with a specific region.

The government can access the flight records of anyone who has flown to or from an airport in the US.

Photos and videos taken from the air above your house and from the street are legal, including satellite and drone imagery.

Biometric information



More avant-garde surveillance focuses on information that can identify a person's physical characteristics. Biometric analysis can be used to identify people based on a photo, fingerprint, or even a retina scan.

If you have a passport, driver's license, or any other government-issued photo ID, then you can be identified by the FBI using facial recognition. In 2017, *The Guardian* reported about

half of adult Americans' photographs are stored in databases accessible to the FBI. About 80 percent of them are non-criminal entries.

The NSA, meanwhile, intercepts tens of thousands of images per day of people's faces. Those images are swept up by bulk surveillance programs that collect the images from emails, messages, social media, video conferences, and other communications, according to a 2014 *New York Times* report.

Advanced security cameras can be placed in transportation hubs like airports and train stations in order to spot and track specific people. As with other forms of bulk surveillance in the US, government agencies are limited to intercepting communications with foreigners or US citizens living and traveling overseas. Domestic communications between American citizens within US borders are legally off limits.

Firearms

The Firearm Owners Protection Act prohibits the US government from creating a national gun registry that keeps track of who owns what firearms. However, the ATF does keep some gun-related databases. These include:

- Sales reports of specific firewarms with owner's name and address
- Guns suspected to be used for criminal purposes but not recovered by law enforcement
- Traced gun records that include the retail purchaser and seller. These include registration records from out-of-business gun stores that incude name, address, make, model, serial number, and caliber
- Guns reported as stolen to the ATF

Bargaining chips

The information age hasn't really changed the types of information that government wants to get its hands on. It just created more vectors for government agencies to get that information, and the amount of information has increased to an exponential degree.

Recall that we've only outlined information that can be accessed without a court order. As you can see, all that info could be coalesced to form a reasonably accurate profile of a US citizen and their behavior. In her article, "A picture of you, in federal data," *Politico*'s Nancy Scola writes:

"Even if the blended data doesn't contain a name or Social Security number, the image that comes into focus can quickly be so specific to plausibly belong to only one person, or a handful of people."

But before you start wheezing into a paper bag, know that Big Brother isn't as smart as he likes people to think. At least, not yet. All of this data is not part of one giant spreadsheet containing every American citizen. It's messy, fractured, and jealously horded. In 2011, political scientist Alon Peled wrote about a top-down order by President Barack Obama to open up federal information caches to the public. The order floundered because, Peled said,

"Datasets are valuable assets which agencies labor hard to create, and use as bargaining chips in interagency trade, and are therefore reluctant to surrender these prized information

assets for free."

So the US government does know a lot about Alice, Bob, and Chris, but it hasn't figured out a way to efficiently manage and utilize that information in cooperation with other agencies. At least, not for now. A single inter-agency searchable database could be a reality in the future.

In 1974, Senator Sam Ervin warned future Americans about surveillance overreach:

"When [the] quite natural tendency of government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators," he said. "The resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive government on behalf of freedom."
