Guidepost

THE SECRET TO PROTECTING YOUR DIGITAL IDENTITY: OPT-OUTS

When I first got into the privacy space several years ago, I had a basic understanding that the biggest, single source "leak" of personal data is the person themself. People were using poor security settings for online accounts, oversharing on social media, and reusing the same username and password for multiple sites. All that made sense. What I was not expecting, though, was just how many different entities are collecting your data without your knowledge/awareness.

Let's consider two common government organizations, the United States Postal Service and the Department of Motor Vehicles. Part of the federal and state government respectively, they are organizations that are perceived as pretty much harmless. What most people do not know, is that both the USPS and the DMV (in many, but not all jurisdictions) sell your data.

Think about the type of information they have. The post office knows exactly where you live – that's valuable information for people who want to sell you things. They also know when you move and where you're moving to. Many people who have moved, myself included, have paid the nominal $1 fee to the USPS to forward your mail for six months when you relocate. The irony is, we have actually paid the post office to make our data more valuable to sell!

The DMV, meanwhile, has access to some unique information too: your birthdate, address, height and weight (which can be used to calculate your BMI), if you're an organ donor, and even if you need prescription lenses. I'm sure you can quickly name five companies who could use this information to sell you something. As a matter of fact, you've probably already received their advertisements in your mailbox.

While this is a complex issue, let me try to give you a baseline understanding of what is going on and how to protect yourself. The companies that buy and then sell all this data are called, unsurprisingly, data brokers. One such company, Acxiom (now known as LiveRamp), has profiles on 96% of US households, with each profile containing thousands of data points such as phone number, age, race, political affiliation, heath status, estimated net worth, and more. According to *The New York Times*, they operate over 23,000 servers and collect 50 trillion unique data transactions each year. Oh, and they had a data breach that resulted in the loss of 1.6 billion customer records.

So, is there anything you can do about it? Well, yes. You can opt-out from these data brokers. The challenge comes in knowing where to go and what information to provide. Sometimes it is as straight forward as typing your information into a form and clicking submit, other times it requires sending an opt out request via snail mail using the correct color crayon. I'm mostly kidding about that last point.

A quick Google search will identify several services that claim they can do the opt-outs for you for only a few hundred dollars. Avoiding the obvious conflict for a moment that some of these sites are also run by the same data brokers who are collecting and selling your data in the first place, there is a big caveat people often miss. While yes, they do go and delete your data, it's a singular event. After a few months, all your data is back to being bought and sold and you're out the money.

In our experience of doing opt-outs manually, it takes about six weeks of work to start seeing results, and constant maintenance (e.g., checking that information that has been removed stays removed) for the next six to nine months, which may include going through the opt-out processes again. Additionally, you must concurrently ensure that you are not creating new profiles or data points that can be collected and sold (for example, signing up for a new food delivery app or online shopping portal).

If that seems like more hassle then its worth, well, that's exactly the way it is designed. Yet the results are more than worth it. By removing your personal data from the data brokers, the amount of information out in the digital world is drastically reduced. If you've ever feared being doxed, then this is one way to prevent such an event from occurring. Even those of us with access to proprietary investigative databases become foiled when your information is removed. When things like your utility records, vehicle registrations, and phone number start getting removed from databases, it becomes exceptionally more difficult to positively identify you. Until eventually, with the right lifestyle decisions, you can utterly disappear "on paper."

The first step in protecting your online profile is to conduct a digital vulnerability assessment ("DVA"). This self-due diligence is conducted to understand the universe of information available about you in order to make an informed decision about what information can stay public and what must be private. The DVA often includes data like your home address, personal phone number, email, date of birth, social security number, the vehicles that you drive and their license plates, your political affiliation and immediate family members. Yet this is just the low hanging fruit. Political donations can grant insight into what social causes you support, speaker or alumni bios may provide details on your children, their ages, and where you currently work, Venmo payments (which are public by default) can reveal who you pay and for what. Even online reviews you left about your favorite local pizza shop or personal physician grant clues as to where you may live or what medical conditions you might face. Collating these tiny details is enough for identity thieves to develop a pattern of life, and gain access to your banking information, health records, or impersonate you online to damage your reputation.

Third-party privacy consultants assist by putting you back in control of your data and digital identity. Inform yourself by starting with a DVA and work with an expert to understand what data an opt-out service can remove, and what

additional steps may be necessary to improve your cyber hygiene. Even if you do not want to become a digital ghost, there is something to be said about reducing the amount of those pre-approved credit card offers that junk up your mailbox each week.

CODY SHULTZ PCI, CCI

Director, Investigations + Private Client Protection

Cody Shultz serves as a director of investigations and private client protection for Guidepost Solutions and is based in the D.C. office. Having served with the Central Intelligence Agency, he is now sought out as an expert on reputation and identity management for ultra-high net worth clients and family offices. He holds a Professional Certified Investigator certification through ASIS International and is a Certified Cryptocurrency Investigator.