A University cyberlaw expert explains your 'data exhaust trail' and offers tips for covering your digital tracks

University Communications
January 2023

Living increasingly online comes with a lot of convenience.

Social media keeps friends and families perpetually connected. Streaming a movie is exponentially easier than driving to a movie theater or a video rental store. And ordering groceries on your phone beats a trip to the supermarket most of the time.

But all of these activities come with a “data exhaust trail” — the breadcrumbs of information consumers leave behind when they browse the web — which companies use to tailor ads or otherwise make money, said Derek Bambauer, a professor of internet law in the James E. Rogers College of Law. Bambauer’s research focuses on online censorship, cybersecurity and intellectual property. He also has written technical articles on data recovery, and, before his legal career, worked as a principal systems engineer for Lotus Development Corp., a software company that once was a division of IBM and is now part of HCLTech, an Indian information technology company.

The International Association of Privacy Professionals, which helps organizations protect their data, has dubbed Jan. 28 Data Privacy Day — “an international effort to create awareness about the importance of respecting privacy, safeguarding data, and enabling trust” — in partnership with the National Cybersecurity Alliance, which advocates for the safe use of technology and educates people on how to stay safe online.

According to the International Association of Privacy Professionals, the Council of Europe held the first Data Protection Day on Jan. 28, 2007. The occasion marked the day the council opened the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – known as Convention 108 – in 1981.

The U.S. Congress passed its own resolutions in 2009 to recognize National Data Privacy Day, though neither the House of Representatives’ nor the Senate’s resolution acknowledges the shared date with the European Council’s convention.

In this Q&A, Bambauer explains how and why our data gets collected and the laws we have to regulate data privacy. He also provides some practical tips that can help the average online consumer keep their data safe.

“Data privacy” has become a phrase we hear a lot these days, but what does it actually mean?

If I had to give a bumper-sticker definition, I tend to think of data privacy as meaning control over information that you don’t want to be universally shared. Examples might be my health status, in some cases my age and there might be some instances where I don’t want my name disclosed.

The classic model of privacy is: “Once I give it up, it’s kind of out there, it’s free to others to use.” So, the whole notion of privacy in some sense is to impose some limits on that, to make it so that I can share information under some circumstance or with some people, but not with everyone.

How does our data typically get collected?

There’s really three ways. Sometimes, we have to reveal data, like when we file a tax return, file an unemployment claim or fill out a credit application with a bank. To exist in the modern world is to have to share data.

There are some times when we voluntarily share data. Social media is a good example: We tell social media companies about ourselves in exchange for a product or service.

And then we also leave sort of a data exhaust trail through things that we do. So, for example, based on the searches that I do on Amazon, Amazon will recommend products to me. Based on the songs that I pick on Spotify, it will curate additional music for me. It’s also possible for apps or websites to see which website you came in from.

Why is our data so valuable to companies?

Usually, it’s because a company wants to do targeted advertising. They want to figure out which products or services you’re more likely to buy, or which ads are more likely to attract your attention. Advertising is by far the biggest piece of it because the modern web economy runs on advertising. It’s how companies like Google and Facebook make money.

There’s also a massive industry that we commonly refer to as data brokers whose function is to simply aggregate data about you from multiple sources, and then either use it directly or sell it to third parties. I think that’s one of the areas where people become more concerned because it’s fine for me if my employer knows if I’m on a particular health plan, if they know what pharmacy I use so they can reimburse them, or if the pharmacy knows what prescriptions I take. But I might be really uncomfortable if the pharmacy shared the prescription information with my employer.

So, in some senses, one of the things we want with data privacy is the ability to build walls between certain types of information.

What are the current federal U.S. regulations that deal with data privacy?

The United States, for better or worse, has a model where we tend to have sector-specific legislation.

Health care has a particular set of rules, passed in 1996, as part of the Health Insurance Portability and Accountability Act, or HIPAA, that do things like mandate privacy and security for personally identifiable information in a health context. There’s a weird set of protections in areas like driver’s license information. There are protections for your video rental records, back when Blockbuster was a thing. The financial industry has a certain set of regulations. The Family Educational Rights and Privacy Act, FERPA, is another good example.

All of these things are basically individual silos, which means that whatever expectations of privacy we have are really tied to the type of data, and that might not track with people’s intuitions.

The Federal Trade Commission has sort of become the de facto privacy enforcer for the United States under a relatively broad statute that authorizes it to deal with unfair or deceptive acts or practices. So, the FTC has jumped in in a big way to regulate online privacy.

Some might assume that younger generations are a little more forthcoming with their data than older generations. Is that generally true?

It is absolutely correct that the generation of digital natives — who are posting to TikTok regularly, taking advantage of social media, all of these things — either are less concerned about privacy or they see the tradeoffs as worth it. So, I think there’s no doubt that there’s just more data revelation with them.

But I would say too that there’s more digital activism among that generation. They are more likely to become active in civic organizations or movements or protests when they think that there has been misbehavior or mistreatment. So, I think there’s a greater tolerance for it, but they’re also more likely to take more action when the lines have been crossed.

Speaking as an internet law expert who’s also a parent, what advice do you have for parents who aren’t sure how to approach protecting their children’s data privacy?

My practical take with parents is, you want to have a conversation with your kid, and you may ultimately have to ask, as the parent, whether there should be social media apps on their phone. What should the usage be? Should it be a Wi-Fi-only phone, or should it be a cellphone? The second thing is, I think there’s a lot of value to monitoring, and maybe more value to monitoring than prevention. Because prevention is really hard, and with monitoring, if you see something going on, you can have a
discussion about it. It's a teachable moment.

What practical data privacy advice do you have more generally, or for University employees?

There are places where you can certainly erase data. You can erase Google's type-ahead feature, you can erase certain histories. But that's one of those tradeoffs: It is useful, so you have to decide what level of risk you're willing to live with. It's also so easy to get free email accounts, so you can sign up for free email accounts so you're not under your real name everywhere.

Some data exhaust is inevitable in this world, so you have to decide whether additional sharing – the loyalty program at the supermarket, whether your social media feed is public – is worth it to you.

At the University, sensitive data is going to have its own set of rules, and we all have to go through the security awareness training [6]. But common sense takes care of a lot of that. If you've got patient health information on your laptop, if you have stuff from a Department of Defense grant on your laptop, you need to take extra precautions [7].

The other thing that I would say is that there are things you can do that are really painless. If you have a laptop, encrypt its hard drive. Use a password manager [8]. Use the VPN, or virtual private network [9], software. Keep your browser up to date. Install the operating system patches. There are a lot of different ways in which you can reduce your exposure to both inadvertent revelation and having people try to take your data. Some of these things are actually pretty easy.

In many ways, what you want to do is avoid being the low-hanging fruit. You want somebody who is looking for something to go on to somebody who is an easier mark.

More University-specific information about data security [10] is available on the Information Security Office website, where visitors can report a potential information security violation [11], report a lost or stolen device [12], and find resources to protect online data [13].

Source URL: https://uaatwork.arizona.edu/dpc/university-cyberlaw-expert-explains-your-data-exhaust-trail-and-offers-tips-covering-your

Links