SHRINKING THE DIGITAL FOOTPRINT

Marketers, employers and creditors can track your private data. But there are ways to limit the exposure. **BY JON ANNE WILLOW**

As denizens of the digital age, we are constantly giving away our personal information online. We know hackers can steal it, especially when we're not careful. It's kind of like parking your car on the street overnight – even though you locked the doors, it's more vulnerable than if it were in a garage.

But what about information we never intended to share? Unbeknownst to you, every encounter with the Internet builds on something called your digital footprint, and it says more about you than would have seemed possible even just a few years ago. But is this just another way for marketers to make personalized offers? Or are you, personally, being watched?

Your digital footprint is made up of bits of information about your online behavior. Marketers, creditors and potential employers can follow you around, tracking you by your IP address, the contents of your clipboard, your physical location and how you interact on social networks. And if you give a site your name or email address or sign in with your Facebook or Google account – boom! – it's a pretty sure bet that your info will be cross-checked against a third-party database, attaching valuable information such as your name, gender, age, income, marital status, educational attainment, where you shop or possibly even your social media connections.

"It's called re-targeting, or re-marketing," says Tom Johnston, vice president of strategy for Milwaukee-based digital marketing firm Ascedia. "A user visits a 'tagged' Web page, which saves a cookie in the user's browser." That cookie tracks everywhere you visit. This is why we keep seeing the same ad for those shoes we didn't buy.

"You are anonymous," assures Johnston. "You're a series of numbers and characters who has either completed actions or not." So later, when you're on a site that shows advertising, "the ad network instantly checks your cookies, and if it finds one of its own, it serves up the appropriate ad."

Nobody's trying to steal your identity in this scenario, so should you care? Privacy in general is a thing of the past, right?

Perhaps, and up to a point. But did you know Facebook activity is already being used by some to determine your creditworthiness? Kreditech, a Germany-based lender, makes the bold claim that "banking as we know it today is dead" and that "algorithms and automated processes are the way to customer-friendly banking." Kreditech looks at more than 20,000 data points for each loan applicant, including how and with whom they interact on social networks. Steer clear of your friends who have poor credit and you've got a better shot at obtaining a Kreditech loan.

This begs the question: Can it possibly be legal to deny credit based on a loony uncle's inane postings to your Facebook page?

Unfortunately, says Christopher Ahmuty, of the American Civil Liberties Union of Wisconsin, the answer is yes.

"In the past, government agencies would protect citizens against such actions," says Ahmuty. "But since the Reagan era, there's been more pressure to not over-regulate corporate interests." The technology, he adds, has leaped ahead of regulation.

"Most of these laws were passed pre-Internet" says Ahmuty. "The Electronic Communications Privacy Act was passed in 1986, when Mark Zuckerberg was 2."

Johnston and Ahmuty are adamant that consumers themselves do more harm with lazy habits than any data tracker is currently capable of inflicting. Below, they offer simple tips to minimize your digital footprint.

Ahmuty says people need to be careful about what kind of information they offer up via social media. "Resist the temptation to get involved in 'liking' everything. It doesn't really have any value for you, but it's valuable to marketers and creditors." ■

STAY SAFE

Tips to keep hackers at bay.

➜ Block cookies or clear your history after you browse. ➜ Don't save your passwords or store them in a digital document. ➜ Don't copy and paste your passwords into your browser. ➜ Don't use a public computer to log into a secure site. ➜ Don't log in to any account from a public wireless network. ➜ Increase your privacy settings. ➜ Consider reputation management software. ➜ Install a free browser plug-in like Ghostery that blocks trackers. ■

Illustration by Chris Gash