



Data Privacy Detective Podcast – Episode 52: Data Brokers, How Our Personal Information Is Sold

Sep 01, 2020

Categories:

[Blogs](#)

[Podcast](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

Robo-calls, phishing, identity theft, ads we didn't ask for – and worse. How does this happen? How does our personal data get collected, used and sold, without our knowing approval? Data brokers are the primary answer. They are businesses that collect, use, and sell blocks of personal information to a wide variety of buyers. This is not per se a shady business, though it may seem that way to those of us overwhelmed with constant interference by phone, email, pop-ups, and attacks aiming to disrupt our day or steal our assets or identity.

[Rob Shavell](#), CEO and co-founder of [Abine](#), a 10-year-old privacy company, gives us a tour of data brokerage. Our personal data is collected in many ways. Some is virtually public – postal address, registered voter information, other ways in which details about us become publicly available. A lot of information about ourselves we contribute to the world – through social media posts, publicity, items we publish. There's a tension between our instinct for privacy and the desire to be known, even famous if only for a day or two. Sensitive information is held by financial institutions, healthcare providers and others, who are generally restricted by federal and state law from sharing it with others but are themselves victims of a data breach. Information once disclosed becomes available to data brokers, who organize, package and sell the data to others interested in advertising to customers, monitoring behavior, analyzing groups or otherwise seeking data for their legitimate purposes (and otherwise).

Enter Vermont. A 2019 statute required data brokers to register with its Secretary of State. 121 data brokers did so by March 2019. While the state did not require brokers to disclose what data they were collecting, buying or selling, it exposed the extent of the data brokerage industry willing to reveal itself to deal legally with Vermont residents' data, and it gave individuals the ability to opt-out of data broker systems of those that offer one.

It is less understood that credit rating agencies, for example, may share our personal data with third parties – unless we instruct them not to. Aside from medical, financial and a few other categories, there is no U.S. federal law restricting businesses from selling our information to third parties. U.S. persons generally must “opt-out” from the privacy policies businesses post to permit such data sharing, policies few of us ever read. Many businesses make it difficult to opt-out of allowing data sharing. As a 2019 Wired article quoted Joseph Tomain of Indiana University’s Center for Applied Cybersecurity Research, “Theseus had an easier time escaping the Minotaur” than Amazon allows a user to stop Alexa from share our personal data with strangers.

And there’s the dark side – information sold or resold to hackers, ransomware artists and other nefarious forces who use our personal data to steal from us, from employers, from financial institutions and from the government. A client recently was astonished to receive a letter from the Ohio Government unemployment agency informing him that he had filed a claim for unemployment compensation from his own wholly-owned company. Guesstimates of losses from identity theft, ransomware, data breach and other data related fraud range globally up to \$1 trillion a year, just one of countless examples of criminal elements taking advantage of COVID relief funds through fictitious filings for funding, enabled by their use of purloined personal information about us.

What to do? Companies like Abine offer tools to protect individual data, such as Blur and DeleteMe. There are online guides listing opt-out procedures, such as Harvard University’s Berkman Klein Center for Internet and Society, or the Data & Marketing Association’s DMAchoice program (used by some businesses to remove customers from their lists and primarily designed to opt-out of unsolicited direct mail and email messages). Protected persons, such as victims of domestic violence or stalking, can use programs in some states to have themselves removed from contact information with databases through a single request (see the guide to data brokers of the National Network to End Domestic Violence). These and many other offerings provide low-cost efficient means of opting out of third-party data sharing and of making it difficult for personal information to become available to data brokers in the first

place. Cybersecurity firms offer tools to secure personal data from unauthorized theft.

It is for each of us to take prudent steps to limit data loss or unwanted sharing. This includes deleting unnecessary apps, using tracker blockers and browsers with ad blockers, adjusting privacy settings so as not to allow wholesale 24/7 sharing by default settings on smartphones, using privacy tools like a VPN, and otherwise limiting what you post online. Once posted, those words and numbers turn into 0's and 1's that cannot be ripped up like a sheet of paper. As I close each podcast, protecting your personal data begins with you.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.