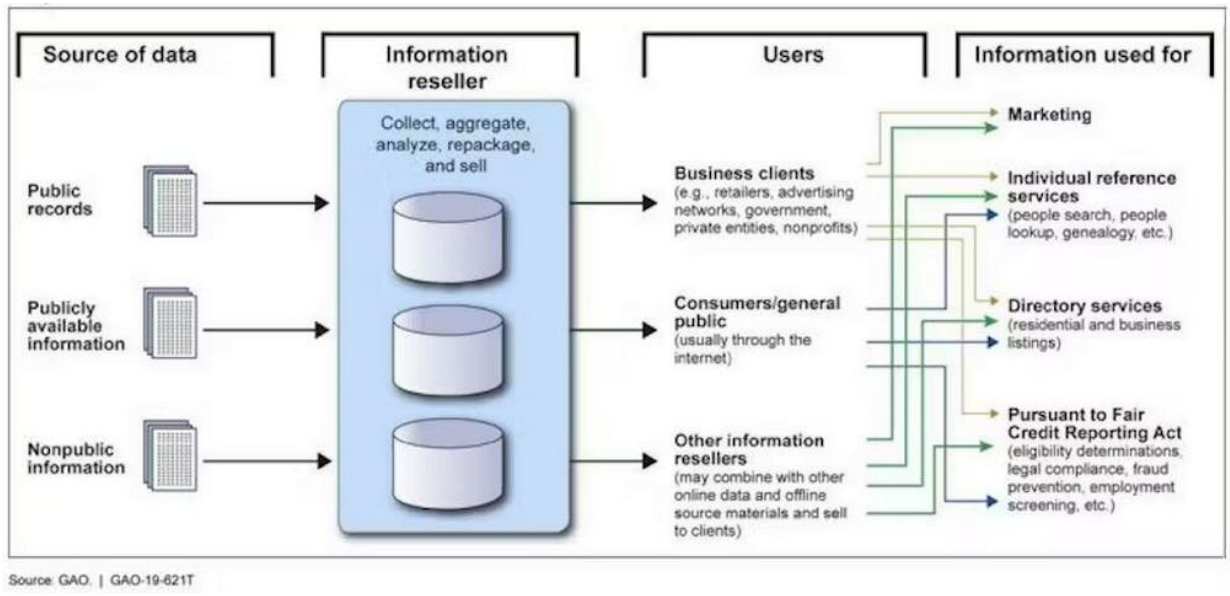
US agencies buy vast quantities of personal information on the open market—what it means for privacy in the age of AI

June 29 2023, by Anne Toomey McKenna



The commercial data market collects and packages vast amounts of data and sells it for various commercial, private and government uses. Credit: Government Accounting Office

Numerous government agencies, including the FBI, Department of Defense, National Security Agency, Treasury Department, Defense Intelligence Agency, Navy and Coast Guard, have purchased vast amounts of U.S. citizens' personal information from commercial data

brokers. The revelation was published in a partially declassified, internal Office of the Director of National Intelligence report released on June 9, 2023.

The report shows the breathtaking scale and invasive nature of the consumer data market and how that market directly enables wholesale surveillance of people. The data includes not only where you've been and who you're connected to, but the nature of your beliefs and predictions about what you might do in the future. The report underscores the grave risks the purchase of this data poses, and urges the intelligence community to adopt internal guidelines to address these problems.

As a privacy, electronic surveillance and technology law attorney, researcher and law professor, I have spent years researching, writing and advising about the legal issues the report highlights.

These issues are increasingly urgent. Today's commercially available information, coupled with the now-ubiquitous decision-making artificial intelligence and generative AI like ChatGPT, significantly increases the threat to privacy and civil liberties by giving the government access to sensitive personal information beyond even what it could collect through court-authorized surveillance.

What is commercially available information?

The drafters of the report take the position that commercially available information is a subset of publicly available information. The distinction between the two is significant from a legal perspective. Publicly available information is information that is already in the public domain. You could find it by doing a little online searching.

Commercially available information is different. It is personal information collected from a dizzying array of sources by commercial

data brokers that aggregate and analyze it, then make it available for purchase by others, including governments. Some of that information is private, confidential or otherwise legally protected.

The sources and types of data for commercially available information are mind-bogglingly vast. They include public records and other publicly available information. But far more information comes from the nearly ubiquitous internet-connected devices in people's lives, like cellphones, smart home systems, cars and fitness trackers. These all harness data from sophisticated, embedded sensors, cameras and microphones. Sources also include data from apps, online activity, texts and emails, and even health care provider websites.

Types of data include location, gender and sexual orientation, religious and political views and affiliations, weight and blood pressure, speech patterns, emotional states, behavioral information about myriad activities, shopping patterns and family and friends.

This data provides companies and governments a window into the "Internet of Behaviors," a combination of data collection and analysis aimed at understanding and predicting people's behavior. It pulls together a wide range of data, including location and activities, and uses scientific and technological approaches, including psychology and machine learning, to analyze that data. The Internet of Behaviors provides a map of what each person has done, is doing and is expected to do, and provides a means to influence a person's behavior.

Better, cheaper and unrestricted

The rich depths of commercially available information, analyzed with powerful AI, provide unprecedented power, intelligence and investigative insights. The information is a cost-effective way to surveil virtually everyone, plus it provides far more sophisticated data than

traditional electronic surveillance tools or methods like wiretapping and location tracking.

Government use of electronic surveillance tools is extensively regulated by federal and state laws. The U.S. Supreme Court has ruled that the Constitution's Fourth Amendment, which prohibits unreasonable searches and seizures, requires a warrant for a wide range of digital searches. These include wiretapping or intercepting a person's calls, texts or emails; using GPS or cellular location information to track a person; or searching a person's cellphone.

Complying with these laws takes time and money, plus electronic surveillance law restricts what, when and how data can be collected. Commercially available information is cheaper to obtain, provides far richer data and analysis, and is subject to little oversight or restriction compared to when the same data is collected directly by the government.

The threats

Technology and the burgeoning volume of commercially available information allow various forms of the information to be combined and analyzed in new ways to understand all aspects of your life, including preferences and desires.

The Office of the Director of National Intelligence report warns that the increasing volume and widespread availability of commercially available information poses "significant threats to privacy and civil liberties." It increases the power of the government to surveil its citizens outside the bounds of law, and it opens the door to the government using that data in potentially unlawful ways. This could include using location data obtained via commercially available information rather than a warrant to investigate and prosecute someone for abortion.

The report also captures both how widespread government purchases of commercially available information are and how haphazard government practices around the use of the information are. The purchases are so pervasive and agencies' practices so poorly documented that the Office of the Director of National Intelligence cannot even fully determine how much and what types of information agencies are purchasing, and what the various agencies are doing with the data.

Is it legal?

The question of whether it's legal for government agencies to purchase commercially available information is complicated by the array of sources and complex mix of data it contains.

There is no legal prohibition on the government collecting information already disclosed to the public or otherwise publicly available. But the nonpublic information listed in the declassified report includes data that U.S. law typically protects. The nonpublic information's mix of private, sensitive, confidential or otherwise lawfully protected data makes collection a legal gray area.

Despite decades of increasingly sophisticated and invasive commercial data aggregation, Congress has not passed a federal data privacy law. The lack of federal regulation around data creates a loophole for government agencies to evade electronic surveillance law. It also allows agencies to amass enormous databases that AI systems learn from and use in often unrestricted ways. The resulting erosion of privacy has been a concern for more than a decade.

Throttling the data pipeline

The Office of the Director of National Intelligence report acknowledges the stunning loophole that commercially available information provides

for government surveillance: "The government would never have been permitted to compel billions of people to carry location tracking devices on their persons at all times, to log and track most of their social interactions, or to keep flawless records of all their reading habits. Yet smartphones, connected cars, web tracking technologies, the Internet of Things, and other innovations have had this effect without government participation."

However, it isn't entirely correct to say "without government participation." The legislative branch could have prevented this situation by enacting data privacy laws, more tightly regulating commercial data practices, and providing oversight in AI development. Congress could yet address the problem. Representative Ted Lieu has introduced the a bipartisan proposal for a National AI Commission, and Senator Chuck Schumer has proposed an AI regulation framework.

Effective data privacy laws would keep your personal information safer from government agencies and corporations, and responsible AI regulation would block them from manipulating you.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: US agencies buy vast quantities of personal information on the open market—what it means for privacy in the age of AI (2023, June 29) retrieved 27 April 2024 from https://techxplore.com/news/2023-06-agencies-buy-vast-quantities-personal.html