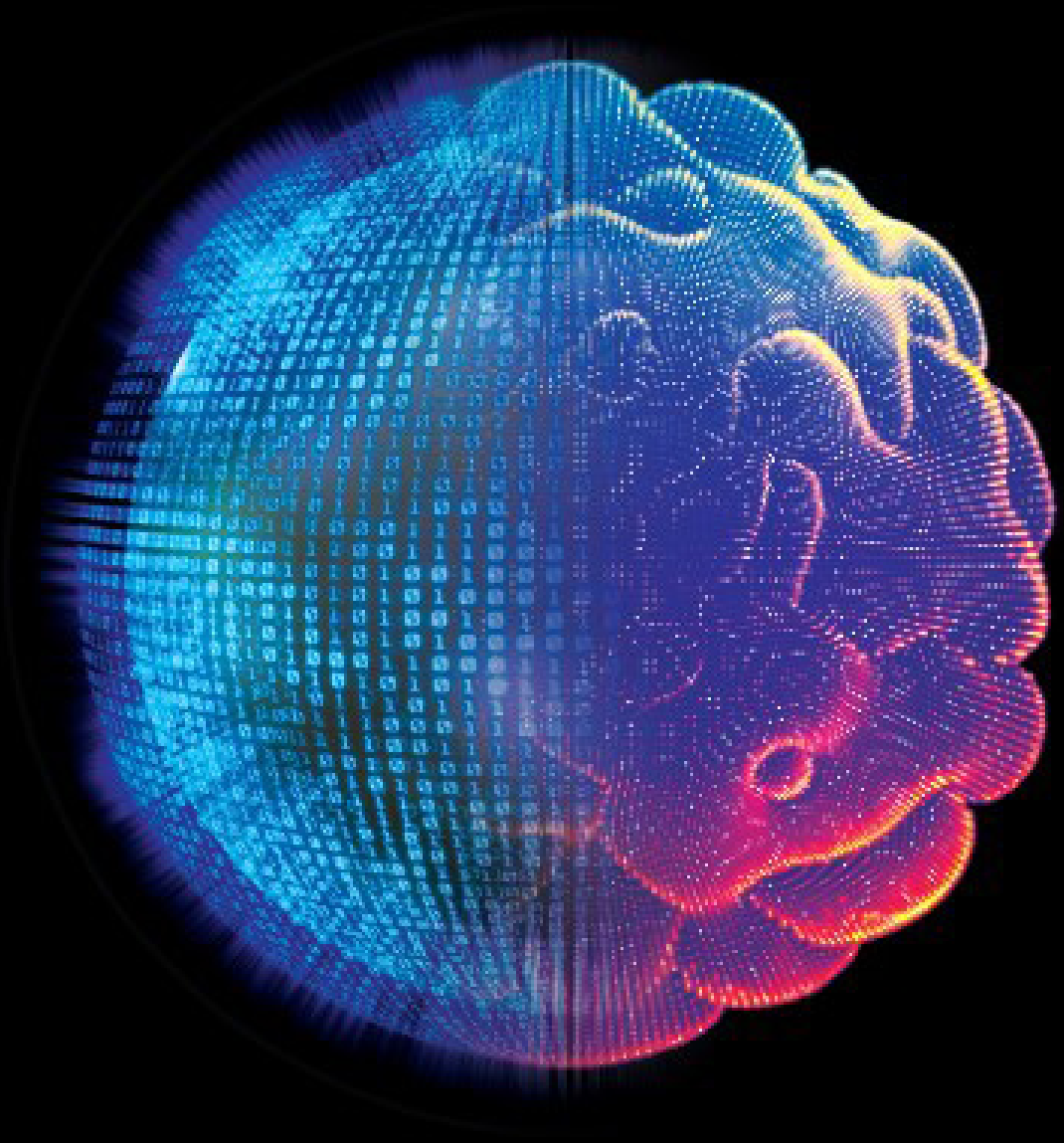
Deloitte.



Five questions about the misuse of consumer data

Five questions about the misuse of consumer data

Recent headlines have shone a spotlight on the potential misuse of consumer data. At center stage are major aggregators of consumer data such as brands, retailers, social media companies, and even government agencies.

However, the reality is that any organization collecting data about consumers—especially if they share the data with third parties—may be at risk of having their data misused. And sweeping legislation such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act means that the days of organizations relying on passive measures, such as terms of service, may be drawing to a close.

If your organization collects, maintains, and/or shares consumer data, here are five questions you should be asking:

1 What consumer data are we currently collecting?

Despite all the ink that's been devoted to the subject of big data, it can be eye-opening to discover just how much consumer information flows through the typical organization. Part of the challenge is that there are so many places data can come in, and so many forms it can take.

Consumers provide much of this information directly, such as when they open a customer account, register a product, subscribe to a newsletter, or respond to an opinion survey. They also provide data informally through email, text messages, posts to the organization's social media pages, and more. Note that consumers may part with some pieces of information more willingly than others. For example, they might not want to give up personal details such as their mother's maiden name, the year they graduated high school, or the name of the street they grew up on—but often they must in order to access their account online.

Then there's data consumers may not even realize they're providing. The organization's public website may set cookies on visitors' computers to track preferences such as language or location. Website logs track users' page visits by URL, time, data, type of browser used, and more. If the user visits while logged into their customer account, they may be personally identified with this information. If your organization has an app for consumers to install on their phones, it may require access to the camera, contacts, geolocation data, and other information. The app also might capture diagnostic and usage data for analysis within your organization.

As internet-connected consumer devices proliferate, they account for an ever-larger share of behind-the-scenes data gathering. Home products from thermostats and refrigerators to lighting and speaker systems transmit data that can reveal a great deal about the consumer's schedule and habits. Finally, there's consumer data that comes in from outside organizations: think credit agencies for customer financing, public records for market research, and contact lists for lead generation.

2 Who do we share the data with?

Organizations often sell some of the consumer data they collect, such as to an ad network or data broker. Even if it doesn't sell its data, the organization might make it available to trading partners, researchers, marketing firms, or other parties with whom they collaborate. Consumer data also can end up with government entities of various jurisdictions.

Some of these uses may be innocuous or even required under the law. Others? Not so much. Consider the organization that distributes to consumers an app containing a GPS tracker. The organization then turns around and sells the GPS data from the app to an insurance company that uses it to profile consumers' driving habits. That outcome may have nothing to do with what the consumers thought they were agreeing to when installing the app your organization provided.

Beyond that, authorized third parties can use consumer data in ways your own organization doesn't intend. Let's say your organization shares consumer data with an academic institution to help it conduct cancer research. That institution then uses your data for medical research only tangentially related to cancer and sells the findings to a global pharmaceutical company. That wasn't the purpose of the study you were supporting, but your organization ended up having a hand in this data-sharing anyway.

And in some respects, organizations are as vulnerable as consumers when it comes to sharing data unintentionally. For instance, web browser extensions may capture consumer information from whatever the employee is working on, be it project materials, medical records, tax returns, passenger manifests, or something else. Another example is apps that external vendors develop on your organization's behalf, which could scrape user data from the social networks to which that consumers belong.

3 How can we determine how third parties are using or misusing the data?

Organization often rely on written terms of service to protect the consumer data they share. Whether this is enough to shield the organization—and its consumers—from excessive risk is debatable. Certainly, companies insist on more proactive security measures when it comes to protecting their trade secrets. A similar approach may be appropriate for consumer data, especially in the current climate.

Admittedly, many organizations have limited visibility into what happens to the consumer data they share. They may not know what fields or attributes the third party is accessing, nor even what kind of consumer information it is (e.g., metadata). Take "data pulls," for example. Organizations may be able to see who is extracting data from their centralized databases, but have a harder time tracking the data after that. For instance, the data could be moved into a different, newly-created internal database first, then go to an outside party.

Getting on top of this requires situational awareness. It starts with a thorough understanding of the company's business model and tracing how data travels from one point to another. Or it could involve reverse engineering the process, starting with the output third parties are using and working backward to discover where it may have originated within your organization. Either way, the technology exists for an organization to monitor what is happening with the customer data in its care.

4 What actions can we take if we suspect the data is being misused?

Once suspected misuse takes place, an organization's options are often limited. A common response is to carry out an audit. Organizations should embed the right to a broad-based audit into the contract they use when selling consumer data to or otherwise sharing data with a third party. Otherwise, they may find themselves in the position of having to ask for the third party's cooperation, and potentially being turned down.

But an audit depends on the third party's disclosures and can only confirm whether those disclosures are in compliance with established data privacy and security standards. In other words, data audits are like locks on doors—they discourage casual misuse, but probably won't stop a determined bad actor. To identify misuse, organizations should undertake a full-fledged investigation so they can understand the intent. And to investigate, organizations generally have to initiate litigation.

Modern forensic investigations are formidable. They involve the use of advanced and predictive analytics to reconstruct how data misuse occurred within the third-party organization. Forensic investigators are trained in interrogating witnesses, uncovering evidence, and translating complex information into lay terms should the case go to a jury trial. That said, such investigations should be considered a valuable extension of, rather than replacement for, a robust program of security and privacy controls.

5 How can we improve governance and controls around consumer data?

First, it's worth asking whether your organization should even have some of the consumer data it collects. This may sound counterintuitive—after all, organizations are constantly urged to create a personalized experience for consumers, and data is a key to effective personalization. Still, it's entirely possible to gather more information than necessary for that purpose. It's also possible that some of the data you have may has outlived its utility. Appropriately and defensibly disposing of that data, or not collecting it in the first place, may reduce your organization's exposure to risk.

A related question is what constitutes a legitimate use of consumer data. That includes inferring additional information from the data that already exists. This has become a significant risk now that widely available technology can rapidly scan and draw connections among even unstructured data. Suppose a streaming video company were to share consumers' viewing habits: Could analytics reveal those consumers' likely age, gender, or race? And if so, what are some ways that information could be misused? It is important for stakeholders within organizations to think through all the ways such scenarios could play out and let that inform the permissions they extend for use of their consumers' data.

Finally, organizations should map all the stores of consumer data in their organization. That includes more than just finding out where it all resides. It also means knowing how the data is secured, who has access, how it can be retrieved, and how it moves through the organization from sourcing to disposal. Automated data mapping tools can help to make this task manageable. Meanwhile, a commitment to treat consumer data like borrowed property helps to keep the goals of a governance program in perspective.

Our take

Organizations that collect consumer data should consider how they interact with their vendors or other third parties. If they share their consumer data with those third parties, it's important to understand what's at stake. It's not just the type of data and whether it's subject to privacy laws—it's also the different ways third parties could misuse the data, either intentionally or inadvertently. In this light, organizations should treat the consumer data in their care as they would their own so they can reduce financial, regulatory, and reputational risk.

Contacts:

Satish Lalchand
Principal
Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
+1 202 220 2738
slalchand@deloitte.com

Mike Weil
Managing Director
Deloitte Financial Advisory Services LLP
+1 312 486 0207
miweil@deloitte.com

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this article.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2019 Deloitte Development LLC. All rights reserved.