Keeping Tabs: Understanding Online Data Privacy (May 2023)

As we learn from the business world, we want to share that information with our community of educators and business professionals. Recent focus panels, news articles, and public policies have raised the issue of data privacy and its increasing relevance in the digital age. The following Action Brief explains challenges and dilemmas surrounding data privacy, as well as what steps companies and lawmakers are taking to better protect personal information online.

The Data Economy

You may have heard this saying before: "If something is free, YOU are the product."

The internet is the ultimate example of this motto in action. While many online services, namely social media and search engines, may be free to use, the trade-off is that these sites collect and sell your personal information to other companies. These companies purchase massive amounts of data—everything from location to search history—and personalize product advertisements based on this information. Commonly called the *data economy*, this multibillion-dollar industry is projected to double in size by 2030…all revolving around the buying and selling of consumer information.

Unsurprisingly, this massive marketplace has led to concerns about the privacy of individuals' online activities. High-profile examples of data privacy leaks and scandals—such as the Facebook–Cambridge Analytica lawsuit and the Yahoo Data Breach—have intensified calls for the regulation of online data collection. But beyond the infamous instances of data privacy failures, the growing power of the data economy has many worried that people's right to privacy will be permanently altered.

The Legal Landscape

The main issue with online data regulation is, in the words of *The New York Times*, "currently, privacy laws are a cluttered mess of different sectoral rules." Rather than a comprehensive federal law that sets uniform guidelines for online data use, there are "smaller" laws that protect specific categories of data (like financial or health information) or specific demographics (like children). This labyrinth of legislation creates confusion for individuals and businesses, and it can open the door for bad actors to exploit those who are uninformed.

There are still some privacy laws that could potentially be adapted to the federal level in the United States. The General Data Protection Regulation (GDPR) is a comprehensive data privacy and security law by the European Union. The GDPR imposes strict requirements, such as requiring businesses to allow consumers to access and review any data collected from them. There are also several state laws that seek to implement comprehensive data privacy regulations, such as the California Privacy Rights Act (CPRA) and the Colorado Privacy Act (CPA), which goes into effect on July 1, 2023. Connecticut, Utah, and Virginia have also created privacy laws that will take effect in 2023.

The Role of Businesses

Ultimately, companies are responsible for ethically collecting and distributing user data. It falls to individual businesses to hold *themselves* accountable—not just because legislation is in its infancy, but because most people continue to use digital services despite growing concerns about data privacy.

According to a KPMG survey, 86% of U.S. citizens say data privacy is a growing concern for them, and 40% of U.S. citizens don't trust companies to use their data ethically. However, use of social media, SVOD (streaming video on demand) platforms, and e-commerce continues to increase among the general population.

This might seem contradictory, but considering how universal online usage has become, combined with how confusing and tiresome privacy procedures can be (think about all the terms and conditions you quickly scrolled past before pressing "Agree"), it's easy to see why there is a disconnect.

So how can businesses handle consumer data responsibly? There are some core principles all tech companies can follow:

- **Employee training and compliance.** The fact that data privacy policies and laws are complicated isn't just a problem for consumers—it also poses challenges to the employees who must adhere to them. To ensure they have a cohesive data-management plan, there are a variety of best practices businesses can employ.

  The most basic steps a company can take is to keep their employees informed of important company policies and the state or federal laws they adhere to. Participants from a recent digital-marketing focus panel emphasized the importance of this. Panelists shared that entry-level employees are often unfamiliar with basic data privacy laws and regulations, which can lead to legal consequences for individuals and companies. Businesses can also standardize their own procedures and implement quality-control processes to consistently evaluate their practices.

- **Transparency.** With the increasing complexity and fluidity of the digital economy, transparency is perhaps the most important principle tech companies can follow. According to a Consumer Reports survey, 60% of U.S. consumers believe they could make well-informed decisions if businesses were required to be more transparent about their privacy policies.

  Let's look at a company that has been viewed as an industry leader in data transparency: Apple. While not without its own privacy controversies, Apple has maintained a decent track record of offering consumers an honest reporting of how their data is collected and shared. This includes their yearly Transparency Report, which discloses government and commercial data usage, A Day in the Life of Your Data, an educational series that helps users better understand how their data used, and Privacy Nutrition Labels, which explain how different apps in the Apple Store collect and distribute user data.

  Focus panel participants echoed the importance of transparency, especially in the reporting phase of a data breach. Cyber security is inherently tied to data privacy and protection.

- **Obtaining permission.** It may seem obvious, but a crucial step to appropriately handling consumer data is requesting—and respecting—consent from consumers themselves. This means informing users what data is being requested and providing options for them to control what they are willing to share.

Further, companies must *actually* respect the privacy preferences of consumers. In 2022, Google faced several lawsuits for continuing to track users who had changed their privacy settings to turn off location data collection, resulting in a settlement payout of nearly $600 million.

The future of the digital-information economy will be decided by the actions of organizations *and* individuals. While companies should hold themselves accountable for protecting the privacy rights of their consumers, the average digital citizen must also take a more proactive role in safeguarding their own online presence. As the country awaits coherent legislation, think about how you can better understand—and preserve—the privacy of your digital information.

Links for Further Reading:

- Radical Proposal: Data Cooperatives Could Give Us More Power Over Our Data
- Data Privacy Guide: Definitions, Explanations and Legislation
- Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information
- The Impact of Privacy Regulations on Digital Marketing
- 'Shut It Off Immediately': The Health Industry Responds to Data Privacy Crackdown
- How Dark Patterns Mislead You Into Making Bad Privacy Choices

Discussion Questions:

- Do you read a website's Terms and Conditions agreement? Why or why not? Do you consider the implications of accepting the terms without reading them?
- What role does transparency play in data privacy issues? What about fairness?
- What are some possible long-term consequences of companies having unlimited access to their users' data?
- Do you feel confident that effective legislation regarding data privacy will be passed? Do you trust governmental bodies to understand and regulate digital services like social media or search engines?

Sources:

- Capitalizing on the Data Economy
- Global Big Data Industry
- Meta Settles Cambridge Analytics Scandal Case for $725m
- Yahoo Data Breach: What Actually Happened?
- The State of Consumer Data Privacy Laws in the US (And Why It Matters)
- What Is GDPR, the EU's New Data Protection Law?
- Is It Time For a U.S. Version of GDPR?
- California Consumer Privacy Laws
- Colorado Privacy Act (CPA) Rulemaking
- Corporate Data Responsibility

- Are Data Privacy Concerns Driving Consumer Behavior? Not Yet.
- Privacy Front & Center
- 11 Apple Privacy Problems That Might Surprise You
- Apple Transparency Report
- A Day in the Life of Your Data
- Apple Privacy Labels
- Data Privacy Rules Even a Kindergartener Can Understand
- Google Racks Up $600M in Privacy Settlements Across U.S. How Much Will Users Get?
- Customer Data Management—Definitions, Benefits, and Best Practices