**Is it right to give up your rights?**

Jude Lamonth

School of Cybersecurity, Old Dominion University

IDS 300w Term Paper

April 24, 2022

**Abstract**

Do companies have the right to use private user data as an exchange for consumers to use their platform? Private data is the information shared by a consumer with a company for a product or service. The collection and use of private data from customers becomes a major source of revenue for companies. With this being the case, there are some ethical and legal concerns. In this paper, some major concerns are addressed such as the pros and cons to giving up your personal data, ethical queries of consent, user convenience, financial gain of companies, and legal documents in place to protect users from exploitation. Also addressed, is an applicative synopsis of the disciplinary perspectives mentioned above.

**Is it right to give up your rights?**

In today’s society, consumers give up private data in exchange for using a platform. The consumer data allows companies to provide a better service for the user. For example, when a consumer gives their email address, the consumer is allowing the company to send them emails about their orders, special offers, and other company news. In exchange for their email address, the consumer receives their products quickly and without hassle. As an interdisciplinary researcher, it is important to take into account the different contexts and applications of private user data. In this paper, the term “private user data (PUD)” is used to describe the information shared by consumers with a company for a product or service. Privacy is often discussed in the context of a single discipline, such as information theory or computer science. However, privacy is an issue that affects all human beings, not just computer scientists or information theorists. Therefore, an interdisciplinary approach is necessary to fully understand the privacy concerns of private user data. It also allows the researcher to consider the ethical, financial, and legality concerns that consumers have when collecting and using private user data.

**Ethical Perspective**

An ethical framework for private data usage is one that seeks to increase customer value without placing them at greater danger from a company perspective. In an expanding digital world, such a strategy conforms with privacy requirements while always pushing for improvements. In a digital economy, it is more profitable for companies to provide a better service to their customers if they take into account the financial value of their customers’ data. By protecting the privacy of their customers, companies increase their financial value, which can be used to improve their service for their customers. Legal frameworks for the protection of private user data provide a reason to keep companies in check and set parameters on what they can do with the data and what they can’t do.

**Ethics in Regards to Data**

The ethical perspective of data protection and privacy stands out in two ways; data consent and data handling. Out of both perspectives (financial and legal) the ethical perspective ties all other perspectives together. The first concern of data consent is the way that consumers give consent to companies for their private data to be used. Data consent is the process of informing consumers that they are allowing the use of their data and obtaining their consent before its use (Facca et al., 2020). When a company obtains consent, it is considered legally binding. This provides consumers with control over their personal data and helps to protect them from companies using their data without their knowledge or consent. What defines consent is complex and it could vary depending on the company. Some may use the acceptance of terms and conditions as a form of consent while others may explicitly ask for a signature of some kind stating that you are willing to allow the use of data (Lee et al., 2016). The second concern of data handling is the type of data that is handled by companies. The main categories that are considered when defining data handling are sensitive and non-sensitive data. Sensitive data refers to data that could cause harm or distress if it was disclosed to the wrong person such as private user data (name, date of birth, and social security). Non-sensitive data refers to data that does not cause harm or distress if it is disclosed such as the amount of customers a company has or the cost of living in a certain location (publicly available information) (Fletcher, 2022).The handling of private user data is concerned with how companies interact with the data that they have collected. The main way that companies can keep users safe and not cause them harm can be achieved by setting boundaries on how they use data and by only using data for the purpose that was provided. WorldCOM for instance, was one of the largest telecom companies in the late 90’s and early 2000’s (George, 2021). This corporation falsified financial data on income statements and balance sheets to make their business appear more appealing to investors. WorldCom went on to lose these investors billions of dollars through data manipulation, while the corporation racked up nearly $4 billion in accounting fraud. In 2006, they filed for chapter 11 bankruptcy and was later purchased by Verizon (George, 2021).

**Financial Perspective**

The financial reason for the use of private user data (PUD) is to generate revenue. This can be done in a variety of ways such as charging customers a monthly fee for using their service, or selling their private data to third parties. The further that a company is willing to go with the financial reason the more likely they are to be able to generate revenue as long as they are abiding by ethical and legal regulations. Users of a product or service consent to the use of their data. This allows the company to continue to use their data in order to provide a financial benefit to the consumer who wanted their data used in the first place.

**Corporation Financial Involvement**

Numerous internet corporations have acquired personal data using a simple algorithm. They provide a free service to entice customers to contribute personal data. For example, if a consumer consents to the collection of their data by a company, whether that be by the use of a microphone, search engine data, or access to a users photos, the company will use this data to provide them with a relatable product or service that the consumer feels the need to buy further persuading the purchase of item(s)or sell the data to a third party. This type of use results in a positive exploitation of private consumer data. Although this may raise ethical questions, it is evident that there is a financial incentive. According to a recent JPMorgan Chase research study, each individual user's data is worth $4 to Meta's social media company Facebook and $24 to Google (Sen, 2021).

**Benefits and Drawbacks**

Even though this gives a better user experience, there are downsides to giving your PUD to companies and that's being at risk for it being stolen. “Though data breaches can be a national security threat, 86% are about money” (Li et al., 2014). Theft data is used by buyers in a variety of ways. To make fraudulent transactions, credit card information and security codes can be utilized to generate counterfeit cards. Identity thieves can exploit Social Security numbers, home addresses, complete names, dates of birth, and other personally identifying information. The easier it is to steal a sort of data, the more likely it is to be targeted. If you've been a victim of a data breach, you can take the following actions to lessen the damage: Change your passwords for your accounts and notify credit agencies and other institutions that gather data about you, also including your healthcare provider, insurance company, banks, and other credit card firm (Li et al., 2014).

**Legal Perspective**

The question remains, though, as to why private user data needs to be shared in the first place. Most companies will claim that it’s needed for the services they provide, but in reality, the primary goal is to make a profit. However, by sharing your private data, you’re giving companies the right to use and sell it. This could mean that the data will end up being sold to the highest bidder, which could mean that it will be used in ways that you never agreed to. In the United States, the legal reason for a private user’s data is to improve the product or service. In many instances, including retail and financial services, the legal reason for a private user’s data is to provide a better experience for the customer. However, if a user is not fully aware of what information is being collected and how it is being used, it is not consent.

**Legal Regulations**

The General Data Protection Regulation (GDPR), defines consent in the context of data as a “freely given, specific, informed and explicit indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, expressly agrees to the processing of personal data relating to him or her” (General Data Protection Regulation, n.d.). In the United States, the Federal Fair Credit Reporting Act (FFCRA) outlines the conditions under which a consumer has consented to their information being shared. The Fair Credit Reporting Act (FCRA) requires that companies that receive information about you from a credit reporting agency give you the opportunity to review and dispute information they have about you before it is shared. The FCRA also requires that businesses give you a legal reason for collecting your PUI and that they provide you with a copy of your credit report one year after you initially provided it to the company (Federal Trade Commission, n.d). In regards to general user data, there isn’t a federal law regarding the protection of data but there are some states that do. For example, the California Consumer Privacy Act of 2018 (CCPA) is a state law that requires businesses with stores in California to post a privacy policy that discloses the business’s information collection practices. The CCPA also requires businesses to provide consumers with the ability to opt-out of the business’s information collection practices (State of California Department of Justice, n.d.).

**Application of Disciplinary Perspectives**

The application of disciplinary perspectives in an ethical, financial and legal perspective has significant benefits. It provides a broader understanding of the ethical, legal and financial implications of the decisions that are being made and allows for a more in depth analysis of the data that is being used. An ethical decision, for example, is not just based on the financial and legal aspect, but also on the social, environmental and political impact that it will have. Applications of disciplinary perspectives in the field of finance have been used to study a variety of topics including the impact of misconduct on a company and the cost of fraud to a financial institution. This was mentioned earlier using the telecoms company WorldCOM. But, if done through the proper legal systems that are in place to prevent such atrocities, then companies can benefit from using private user data. As used in an aforementioned example, where customers who do agree to the use/selling of their PUD in exchange for free services and convenience, companies like Facebook and Google will take user data and sell it to third party companies for profit. Those companies make a profit on user information and what they search while the reward that’s received are personalized searches and the ability to socialize with friends and family virtually. The legal frameworks for the protection of private data will ensure that consumers have the right to consent to the use of their data and that companies are complying with the laws when using private data. The legal frameworks for the protection of private data will also ensure that consumers have the right to be addressed and that companies are not exploiting private data in a negative way for financial gain.

**Conclusion**

The goal of this paper was to introduce the different contexts in which the term “private user data” is used and to provide awareness for the ethical, financial, and legal concerns that consumers have when collecting and using private user data. It is important that companies consider the ethics and legality of the data they collect in order to seek profit. In today’s digital world, where our every movement, purchase, and action is tracked, it is crucial that we, as the consumers, consider the privacy concerns of private user data in order to create a safe and secure society for all.

**References**

Facca, D., Smith, M. J., Shelley, J., Lizotte, D., & Donelle, L. (2020). Exploring the ethical

issues in research using digital data collection strategies with minors: A scoping review.

*PLOS ONE*, *15*(8). <https://doi.org/10.1371/journal.pone.0237875>

Federal Trade Commission. (n.d.) *Fair Credit Reporting Act.*

https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act

Fletcher, C. (2022). *Why the ethical use of data and user privacy concerns matter.* Data Decision

Makers.

<https://venturebeat.com/2022/02/26/why-the-ethical-use-of-data-and-user-privacy-concer>

ns-matter/

General Data Protection Regulation. (n.d.). *What is GDPR, the EU’s new data protection*

*Law?* <https://gdpr.eu/what-is-gdpr/>

## George, B. (2021). Fraudulent Accounting and the Downfall of WorldCom. University of South

## Carolina.

https://www.sc.edu/about/offices\_and\_divisions/audit\_and\_advisory\_services/about/news/2021/worldcom\_scandal.php

Lee, W., Zankl, W., & Chang, H. (2016). An ethical approach to data privacy protection. *ISACA*

*Journal*, *6*(1).

Li, C., Li, D., Miklau, G., & Suciu, D. (2014). A Theory of Pricing Private Data. *ACM*

*Transactions on Database Systems,* *39*(4), 1-28.

(Li et al., 2014).

Sen, R. (2021). Here’s how much your personal information is worth to cybercriminals – and

what they do with it. Public Broadcasting Service

<https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it>

State of California Department of Justice. (n.d.) *California Consumer Privacy Act of 2018.*

https://oag.ca.gov/privacy/ccpa

Sumner, S. (2015, August). *You: For sale*. O'Reilly Online Learning.

<https://learning.oreilly.com/library/view/you-for-sale/9780128034231/B9780128034057000035/B9780128034057000035.xhtml#st0010>