

UNC-Chapel Hill

Modeling Tradeoffs of Data-Collection vs. the Value of Privacy

Final Project

Connor Bono

PHIL 698

Kirun Sankaran

3 December 2021

I. INTRODUCTION

In recent decades, facets of the economy, society, and culture have changed notably due to the rapid pace of innovation in technology. These social practices play a pivotal role in contemporary society and the everyday lives of individuals. With the development of new technology, how individuals connect and have autonomy over their privacy has also changed. Traditionally, the outcome of progress is recognized as positive and helpful to societal growth. The explosive growth of the Internet, however, has created controversy among some, as the positive nature of its progress is questioned because of the potential threats to privacy that it can create. While technological innovation is important for promoting long-term economic growth and enhancing citizens' overall quality of life, it can have both positive and negative impacts on social practices, raising ethical concerns about one's right to privacy.

In this paper, the models by which two opposing positions present views on the value of privacy and control and exertion of influence over personal data are explained. Position A argues that the (non-economic) value of privacy outweighs the (economic) value of data collection. In this view, the tradeoff of privacy for economic gain and enhanced features is too large. Position A uses a conceptual model to argue the view that too much information is gathered by private companies. As an adjunct to articulate the tradeoffs that the model conveys, Position A uses the case study of 'Jane'. Position B proposes a contrary view, defending that the (economic) value of data collection outweighs the (non-economic) value of privacy. This position uses the minimalist model of privacy calculus to illustrate that the tradeoffs of privacy are minimal to the socioeconomic benefits that data collection provides. The collection of data benefits the producer economically, at the cost of some privacy intrusion, providing users with the convenience of personalized recommendations based on their history or collected data habits. Position B values

these benefits offered with companies collecting data over their assumed minimal cost of privacy intrusion. Much of the discussion surrounding individuals' desire to maintain influence over their personal data references privacy, trade-offs, and models. By assessing the two positions on this debate, a consensus regarding policymaking can better be achieved.

II. PRIVACY

Privacy can be evaluated from a variety of viewpoints making it a complex value embedded with a variety of complex social practices. Supportive of Position A, Kamleitner and Mitchell claim it is an indisputable fact that privacy is not only personal but interdependent.¹ People are intertwined socially and bond amongst each other through the sharing of information. Because of this, individuals holding information about someone can compromise another's privacy by passing on personal information that may not have volunteered themselves. This feature makes privacy a 'multi-actor phenomenon'. While the value of privacy varies amongst individuals, Position B suggests that absolute privacy is unattainable. Individuals make choices in which they surrender a certain degree of privacy in exchange for outcomes that are perceived to be worthwhile the risk of information disclosure.² This is the privacy calculus model which Position B uses to support the view that the (economic) value of data collection outweighs the (non-economic) value of privacy. The fact that privacy is a widely converted value in American society reflects the importance of individualism in the country's philosophical foundations.³ Position A understands privacy to be interdependent, while Position B understands absolute privacy to be unattainable. Defining privacy is relevant in understanding the models which each position uses to support its view.

¹ Kamleitner, Bernadette, and Vince Mitchell. "Your Data Is My Data"

² Dinev, Tamara, and Paul Hart. "An Extended Privacy Calculus Model for E-Commerce Transactions." p.61

³ Cheng, Cliff. "The Academy of Management Executive"

III. MODELING TRADEOFFS

Through the installation of applications, privacy trade-offs can arise where one person's privacy is unknowingly compromised while another has consented to the data collection agreements. Users of applications are presented with decisions to either provide access to their data in order to benefit from the technology or not to reveal any information thus avoiding the risk of data mishandling and violation of their privacy. The collection of data benefits the producer economically, at the cost of some privacy intrusion, providing users with the convenience of personalized recommendations based on their history or collected data habits. Position A would trade-off fewer features that are provided with data collection (personalized data that enable companies to personalize services and messages) for more privacy and security over their personal information. For Position B, the socio-economic benefits of data collection to producers and consumers outweigh the cost of some privacy intrusion. Position B values the benefits offered by companies collecting data and uses their model to show that the assumed smaller cost of privacy intrusion does not outweigh the benefits that are provided by providing data. Individuals must weigh the benefits from their internet usage and data agreements with the risks associated with a potential privacy violation. As a result of these decisions, the trade of personal data is fueled, meaning that the secure handling of user data can not be guaranteed. Tradeoffs are not only prevalent in modernity but proliferate as new technologies and conceptions of privacy create manners in which privacy may be violated.⁴ This makes the discussion of these tradeoffs increasingly relevant.

In Positions A and B, models are used to represent privacy tradeoffs. Both models are compatible with the aim of realism, and through their use, examples are set for the purpose of a view on privacy/data-collection tradeoffs. These models elaborate and use concepts in ways that

⁴ Pozen, David E. "Privacy-Privacy Tradeoffs." p.224

promote coherent understanding for their respective position. Position A uses a representational model to frame the notion that the increasing prevalence of data gathering poses a great concern for the public.⁵ Position B uses a social choice model of privacy calculus to support its original position. The model is used to probe and induce coherence among the various components by introducing that much of individuals' perceived risk is based on privacy control, trust, and privacy concerns. This leads to the conception of how much information individuals should share online. Position B believes that securing privacy on one margin can affect privacy on another margin.⁶ Models play the role of analogizing subjects to criticize and justify a phenomenon and are composed of a structure and an interpretation of that structure.⁷ Position A uses its model to show that with current data-collection practices privacy is under attack more than ever, while Position B uses the privacy calculus model to show the interpretation that privacy is often privileged over the common good.

POSITION A MODELED

Proponents of Position A believe that companies should be more transparent to the public with their data collection, retention, and management practices. Position A takes the view that current data protection efforts fall short in preventing interdependent privacy breaches. This view understands the issue of how much control individuals should have over their data as one where private data is an integral part of governance needed to address privacy policies. Position A aims to be proactive in policy to protect consumers in the future, rather than reactive to sudden changes and threats to individuals' right to personal privacy. In this view, as the commercial use of personal data becomes a growing aspect of business modeling in firms, the need to address

⁵ UNCTAD *"The Impact of Rapid Technological Change on Sustainable Development."*

⁶ Pozen, David E. *"Privacy-Privacy Tradeoffs."* p.224

⁷ Weisberg, *"The Anatomy of Models"*, p.1

privacy policies becomes more important.⁸ Using a three-step model of first identifying the phenomenon of a problem (P), explaining insights from the problem (I), and suggesting solutions to reduce failures (S), Kamleitner and Bernadette identify support for Position A. Figure A is a representational model that can be applied to Position A to frame the notion that the increasing prevalence of data gathering poses a great concern for the public. The figure illustrates situations regarding infringement. A situation qualifies as an infringement when the others have not consented to recipients receiving their goods.⁹ Because the goods are transferred through the sharer, the sharer is key to whether the data transfer happens at all, and whether the others have the opportunity to consent. Kamleitner and Mitchell's model supports the (non-economic) value of privacy over the value of data collection through services.

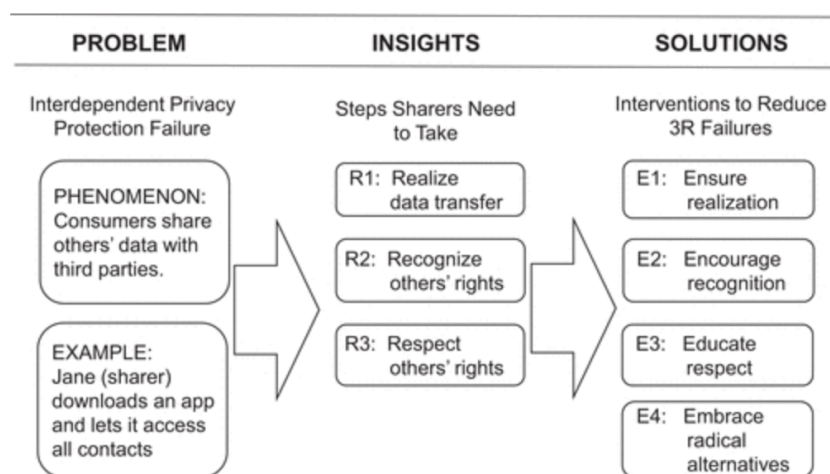


Figure A: Problem's, Insights, Solutions of IPPR¹⁰

Reflective of Position A, Kamleitner and Mitchell introduce the case of Jane to illustrate the problem of interdependent privacy protection failure. Jane represents any consumer who wants to download an app that requests access to data that may concern others. Jane wants to

⁸ Chen, Wenhong, et al. "Privacy and Data Management: The User and Producer Perspectives."

⁹ Kamleitner, Bernadette, and Vince Mitchell. "Your Data Is My Data" p. 433

¹⁰ Kamleitner, Bernadette, and Vince Mitchell. "Your Data Is My Data" p. 433

download a weather app. When she installs the app she is granted the app's promised services, but also agrees to its request to access all her contacts as part of the download. With this, Jane agrees to share the personal data of people other than herself.¹¹ Through this example, Kamleitner and Mitchell explain that 'sharers', like Jane, need to take steps of realizing the data transfer, recognizing others' rights, and respecting others' rights. Jane's sole gain was eased access to information about the weather. Because of this, it is unlikely that Jane infringed on her contacts' personal data because of the benefits of infringement, highlighting that the benefits of data collection should not outweigh the value of privacy.

Kamleitner and Mitchell's model identifies Jane's decision with features of the world, connecting it to the real world Cambridge Analytica case where a company received the personal information of more than 71 million people from only 270,000 consumers who installed its app-based quiz on Facebook. The Cambridge Analytica scandal and its aftermath focused attention on privacy issues and data management practices at major private companies like Facebook, Google, and Twitter.¹² Kamleitner and Mitchell's Jane model and the Cambridge Analytica case stress the effects of lack of transparency, accountability, and regulatory frameworks in increasing privacy concerns. Both models suggest Position A, that current data protection efforts fall short. In this view, increases in privacy concerns can be representative of a need to regulate policies further.¹³

Kamleitner and Mitchell use the conceptual model of Jane, to represent the oblivious sharing of other people's personal data for the purpose of illustrating interdependent privacy protection failure. This case is idealized for simplicity realistic representational tool used to help explain why consumers may fail to protect others' personal data, making broader statements on

¹¹ Kamleitner, Bernadette, and Vince Mitchell. "Your Data Is My Data" p. 438

¹² Kamleitner, Bernadette, and Vince Mitchell. "Your Data Is My Data" p. 433

¹³ Chen, Wenhong, et al. "Privacy and Data Management: The User and Producer Perspectives."

why interdependent privacy protection often fails. Kamleitner and Mitchell's three-step model and 'Jane' adjunct aim at the theoretical virtue of simplicity by maintaining a match between the behavior of the target system and the dynamics of the model. Kamleitner and Mitchell's reflection on phenomenon, insight, and solutions in the model argues that it is complete and relevant in all situations which involve addressing concerns to privacy. The simplicity representational ideal of the model allows it to be a model of interest that can be relevantly applied when describing various phenomena regarding how problems of privacy concerns should be approached. Without Kamleitner and Bernadette's model having the aim of simplicity these applications would not be as relevant.

Since the model used by Kamleitner and Mitchell is less theoretical and resembles reality more closely, foreseeing potential objections to the model can be challenging. The suggestion made by the model and view of enacting stricter regulation in terms of data protection guidelines can be objected to by Position B. In this objection, Position B argues that companies may have difficulties and ultimately may be forced out of business if they face strict requirements. If a business's model is based on the sale of personal data gathered from customers, who in exchange receive cheap or free goods or services, that business model will be compromised and services will consequently be reduced if data-protection regulations prohibit personal data from being processed and passed on in any form. The same is true if legal regulations require anonymization of data which makes them less valuable for the mining of commercially pertinent information. Furthermore, acquiring privacy-enhancing technologies can be an expensive investment for private companies. If data protection restrictions are imposed only on some companies by national legislation, they may face a distinct disadvantage compared to their competitors who are not subject to these restrictions.¹⁴ Several factors may make the provision of data-centric services

¹⁴ Buchmann, Johannes A. *Internet Privacy Options for Adequate Realisation* p.23

more expensive, therefore reducing the profits of the companies that offer these services. This rationale is used to explain why some of the tradeoffs of privacy outweigh the benefits that it provides. Prohibiting personal data from being processed and passed on in its entirety, however, is an extreme form of Position A.

A response for Position A in this objection is suggesting such business models that benefit from personalized data collection violate concepts of privacy and freedom. Position A says that the non-economic value of privacy outweighs the economic value of data collection. This is for the reason that individuals can compromise another's privacy unknowingly creating interdependent privacy failure. Position B would respond to this by saying that even if citizens had the skills and systems to manage their own data privacy, they would not have time for its governance.¹⁵

IV. POSITION B MODELED

Position B positions from the viewpoint of benefits, efficiency, and effectiveness pointing to economic consequences and results, whether they be benefits or disadvantages, either for certain economic players or for the whole economy or the state, thus pushing aside considerations of the intrinsic (non-economic) value of privacy as an essential aspect of personal freedom. From this perspective, the freedom to reveal or conceal who you are in various contexts is not negotiable for the sake of economic benefits, whether they be enhanced income generation or lower prices for some or for all.¹⁶ Most individuals are willing to disclose about themselves based on consideration of their perceived benefits and perceived costs. Communication privacy management theory suggests that people believe they have a right to control their private

¹⁵ Obar, Jonathan A. *"Big Data and the Phantom Public: Walter Lippmann and the Fallacy of Data Privacy Self-Management."*

¹⁶ Buchmann, Johannes A. *Internet Privacy Options for Adequate Realisation* p.23

information and create rules about who is denied or granted access to that specific information.¹⁷ The privacy calculus model suggests that people decide how much they want to disclose about themselves based on consideration of their perceived benefits and perceived costs. The theory is based on the assumption that individuals evaluate anticipated benefits and perceived risks in order to make a rational decision regarding the disclosure of their personal data. These theories and models are useful in evaluating deciding factors with regard to how much individuals are willing to disclose their personal life. Typically, when the benefits of sharing one's data outweigh the costs, people are more inclined to share information. Assessing options of perceived cost and benefit with new implementations in the policy could also be.

Privacy calculus can be applied to examining the tradeoffs of data collection in exchange for added features. Researchers have shown that in addition to online data sharing, advantages and disadvantages are weighed before users provide personal information. User must weigh up the benefits he or she expects from their consumption and the risks associated with a potential privacy violation. Figure B below depicts a privacy calculus model for contact tracing apps. The conceptual model shows how privacy control and trust influence the perceived risks which thus influence an individual's intention to use a service.

¹⁷ Buchmann, Johannes A. *Internet Privacy Options for Adequate Realisation* p.23

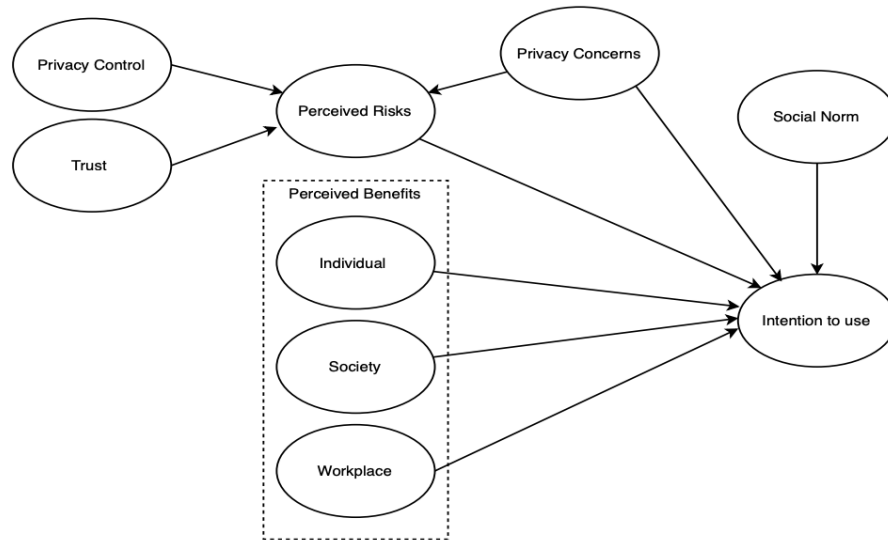


Figure B: Privacy Calculus Model for Contact Tracing Apps¹⁸

As depicted in Figure B, the privacy calculus models suggest that privacy control, trust, and privacy concerns are factors in understanding an individual's perceived risk. Perceived benefits are understood through society, the individuals' and the workplace. Perceived risks, perceived benefits (individual, society, workplace), privacy concerns, and social norms all influence the intention to use.

The privacy calculus model is idealized with the representational ideal of 1-causal. This idealization is meant to make the theory more computationally tractable by assuming that individuals' privacy behaviors are rational. Aiming for completeness and simplification gives a more complete overview of factors pertaining to support on why the benefits of data collection outweigh the risks to privacy. The model is idealized to distort towards assumptions that individuals make fairly rational decisions. Consumers often lack enough information to make privacy-sensitive decisions and, even with sufficient information, are likely to trade off long-term privacy for short-term benefits.¹⁹ The privacy calculus model aspires to the virtue of

¹⁸ Bonner et al. "The (Lacking) User Adoption of COVID-19 Contact Tracing Apps" p.7

¹⁹ Obar, Jonathan A. "Big Data and the Phantom Public: Walter Lippmann and the Fallacy of Data

“1-causal,” by arguing that the decision to provide personal information and agree to terms and conditions is caused solely by human rationality. The model represents individuals’ privacy preferences and choices as being motivated by rational self-interest. Each individual rationally wishes to make decisions that maximize their utility. They can do so by choosing whether or not to use the services provided by private companies online. No single individual is forced to use these services, but collectively with the increasing relevance of the internet, many do and are unaware of the privacy risks, leading to controversy amongst groups. Human rationality is doing causal work in this model.

Privacy calculus can be criticized by the argument that decisions of individuals might be influenced by behavioral biases such as overconfidence. This criticism explains privacy decisions are usually based on incomplete information, and even if detailed information is available the ability of an individual’s cognitive processing might be limited resulting in an imperfect decision. Gerber et al., however, argue that this decision “might therefore seem irrational to an external observer, but at the same time fairly rational to the decision-maker”.²⁰ Results of numerous studies in different contexts additionally provide strong evidence for the privacy calculus model explaining privacy-related behavioral intention and actual behavior.

Position B could respond to this criticism by claiming privacy concerns do not necessarily have a direct influence on the disclosure of personal data. Studies have shown that individuals showed disclosing behavior and use applications that require sensitive data despite expressions of privacy concerns. This empirical data points to notions of a privacy paradox where there is a difference between general attitudes and concrete behavior. Position B supports ideas that if citizens had the skills and systems to manage their own data privacy, they would still have little time for its governance. Consumers will want to pursue the benefits of digital

²⁰ Gerber et al.. “*A Social Comparison Theory Meta-Analysis 60+ Years On*”. p.6

production without being constrained by the means.²¹ People desire privacy and security but are ultimately unable to provide all of the necessary safeguards for protection.

Under Position B, collection of data is inevitable with society achieving higher organization. This alludes to the notion that as societies reach higher degrees of organization, the mechanisms of social control will inevitably expand. Thus, in this position, to run efficient control systems, a considerable amount of information needs to be collected about participants. In commerce, much of the erosion of individual privacy occurs with the consent of the individual.

V. CONCLUSION

As firms collect, use, and share personal information, people lose control over their personal data. As a result of this, some individuals become increasingly concerned with their online privacy and worry about the possible misuse of their personal information.²² Without a clear definition of privacy, it will be difficult for individuals to advise lawmakers on how to protect the general public. Empirical and theoretical research suggests that consumers often lack enough information to make privacy-sensitive decisions and, even with sufficient information, are likely to trade off long-term privacy for short-term benefits. With the increasing integration of technology in a data-driven environment everyday activities will change where the public sees value and ensure that disagreements in view will multiply in relevance.

The models used for Position A strategically place the issue of interdependent infringement at the forefront. This position takes the stance that individuals lack the proper control over the personal information that they should be given. Position B argues implementing

²¹ Obar, Jonathan A. *"Big Data and the Phantom Public: Walter Lippmann and the Fallacy of Data Privacy Self-Management."*

²² Boerman, Sophie C., et al. *"Exploring Motivations for Online Privacy Protection Behavior"*

a new policy could introduce new challenges to business and shift the areas where privacy is violated. As part of its strategy to explain that the economic value of data collection exceeds the tradeoffs in privacy, Position B frames much of data collection to be voluntary— individuals cooperate with corporate surveillance because it returns convenience, and promises protection.²³ In this view socioeconomic benefits of data-collection to producers and consumers outweigh the cost of some privacy intrusion. Much of data collection is voluntary with individuals cooperating with corporate surveillance because it returns them convenience and promises protection²⁴. While Position A aims for ideals of simplicity and close representation, Position B takes the approach of highlighting causal factors. Arriving at a conclusion that sufficiently satisfies both parties is unlikely, though understanding the models used arguments can be helpful in taking a stance on the position of internet data collection and where individuals stand on the issue.

References

²³ Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*.

²⁴ Schneier, Bruce. “*Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*”.

- Barnes, Susan B. “*View of a Privacy Paradox: Social Networking in the United States: First Monday.*”, <https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312>.
- Boerman, Sophie C., et al. “*Exploring Motivations for Online Privacy Protection Behavior: Insights from Panel Data.*” *Communication Research*, vol. 48, no. 7, 2018, pp. 953–977., <https://doi.org/10.1177/0093650218800915>.
- Bonner, Manus & Naous, Dana & Legner, Christine & Wagner, Joël. *The (Lacking) User Adoption of COVID-19 Contact Tracing Apps - Insights from Switzerland and Germany.*, 2020.
- Buchmann, Johannes A. *Internet Privacy Options for Adequate Realisation*. Springer, Imprint: Springer Vieweg, 2013.
- Cheng, Cliff. *The Academy of Management Executive* (1993-2005), vol. 13, no. 3, Academy of Management, 1999, pp. 120–22, <http://www.jstor.org/stable/4165575>.
- Chen, Wenhong, et al. “*Privacy and Data Management: The User and Producer Perspectives.*” *American Behavioral Scientist*, 2018, p. 000276421879128. <https://doi.org/10.1177/0002764218791287>.
- Dinev, Tamara, and Paul Hart. “*An Extended Privacy Calculus Model for E-Commerce Transactions.*” *Information Systems Research*, vol. 17, no. 1, INFORMS, 2006, pp. 61–80, <http://www.jstor.org/stable/23015781>.
- Garfinkel, Simson. “*Database Nation: The Death of Privacy in the 21st Century*”. 2000.
- Gerber, J. & Wheeler, Ladd & Suls, Jerry. (2017). *A Social Comparison Theory Meta-Analysis 60+ Years On*. *Psychological Bulletin*. 144. 10.1037/bul0000127.
- Kamleitner, Bernadette, and Vince Mitchell. “*Your Data Is My Data: A Framework for*

- Addressing Interdependent Privacy Infringements.*” Journal of Public Policy & Marketing, vol. 38, no. 4, 2019, pp. 433–450.<https://doi.org/10.1177/0743915619858924>.
- Pozen, David E. “Privacy-Privacy Tradeoffs.” The University of Chicago Law Review 83, no. 1 (2016): 221–47. <http://www.jstor.org/stable/43741598>.
- Princi, Evgenia, and Nicole C. Krämer. “*Out of Control – Privacy Calculus and the Effect of Perceived Control and Moral Considerations on the Usage of IOT Healthcare Devices.*” Frontiers, Frontiers, 1 Jan. 1AD, <https://www.frontiersin.org/articles/10.3389/fpsyg.2020.582054/full>.
- Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company, 2016.
- “*The Impact of Rapid Technological Change on Sustainable Development.*” UNCTAD, <https://unctad.org/webflyer/impact-rapid-technological-change-sustainable-development>.