Introductory Readings in Formal Privacy for Economists

John M. Abowd, Ian M. Schmutte, William Sexton, and Lars Vilhuber

2019-05-02

Contents

1 Overview 1

2 Background 2

3 Formal Privacy 2

4 Policy and Official Statistics 3

5 Statistical Disclosure Limitation 4

6 Economics of Privacy 4

7 Value of Privacy and Data Accuracy 4

8 References 5

1 Overview

The purpose of this document is to provide scholars with a comprehensive list of readings relevant to the economic analysis of formal privacy, and particularly its application to public statistics. Statistical agencies and tech giants are rapidly adopting formal privacy models which make the tradeoff between privacy and data quality precise. The question then becomes, how much privacy loss should they allow? J. M. Abowd & Schmutte (2019) argue that this choice ultimately depends on how decision makers weigh the costs of privacy loss against the benefits of higher-quality data. Making progress on these questions requires familiarity with new tools from computer science and statistics, the objectives and policy environment within which statistical agencies operate, along with the economic analysis of information.

We have organized these references into a reading course focused on 10-15 primary references in each of six different topics:

- Formal Privacy
- Policy and Official Statistics
- Statistical Disclosure Limitation
- Economics of Privacy
- Value of Privacy and Data Accuracy

In the remainder of this document, for each topic, we provide a very brief description of the papers in the reading course and why we selected them. In each case, we orient the reader to the key issues, concepts, and tools in each topic. In addition to this reading course, we have also curated a much more extensive list of references, available here.

1.1 Contributing

We encourage interested readers and researchers to use these readings for their classes and training, modifying it as needed. You can fork the source code at https://github.com/labordynamicsinstitute/privacy-bibliography.

This document is licensed under the Creative Commons Attribution-NonCommercial 4.0 International Public License (CC BY-NC 4.0). Should that license not meet your needs, contact us to discuss possible modifications or exemption. Please send us any improvements, corrections, or other contributions, either by e-mail, or via the "Issues" feature on Github.

1.2 Support

We gratefully acknowledge the support of Alfred P. Sloan Foundation Grant G-2015-13903 and NSF Grant SES-1131848.

1.3 Disclaimer

The views expressed in this paper are those of the authors and not those of the U.S. Census Bureau or other sponsors.

2 Background

We start by providing a short list of background references that frame a particular set of research topics. J. M. Abowd & Schmutte (2019) show how to combine formal privacy models with the classic theory of public goods to understand and guide decisions about privacy protection and data dissemination. For the neophyte, Wood et al. (2018) provide a non-technical introduction to formal privacy models in general, and differential privacy in particular. Heffetz & Ligett (2014) also introduce differential privacy, but targeted toward economists. After reading these introductory treatments, you should review the textbook treatment of differential privacy in Dwork & Roth (2014) , focusing on Chapters 1–3. We also recommend consultation of the very fine tutorial "Differential Privacy in the Wild: A tutorial on current practices and open challenges" by Michael Hay, Xi He, and Ashwin Machanavajjhala.

To provide a concrete grounding in practical issues of privacy, Jones (2017) summarizes the history of privacy breaches and privacy protection in the U.S. statistical system. It is important to ask how formal privacy models do, and do not, capture common language and legal interpretations of privacy. As such, we also recommend a review of some of the laws governing data privacy in the U.S. , e.g. 13 U.S. Code (1954) and H.R.4174 (2018) (Confidential Information Protection and Statistical Efficiency Act, also known as CIPSEA). A quick review of the Harvard Privacy Tools website (Harvard University Privacy Tools Project, 2019) can provide a sense of how differential privacy is being implemented in various settings. Goroff (2015) also provides a very useful overview of the key issues in this reading course for a lay audience. J. M. Abowd (2017) and J. M. Abowd (2016) survey formal privacy systems being implemented at the Census Bureau.

3 Formal Privacy

The literature on formal privacy is vast. Here, we focus on those papers that will help orient the reader to the key ideas and tools of differential privacy, particularly those relevant to the economic problem of determining optimal privacy protection when publishing population statistics. For the purpose of this reading course and associated bibliography, we associate formal privacy as a literature emerging in computer science out of cryptography. In the section on "Statistical Disclosure Limitation", we recommend additional readings from the SDL literature, which has a distinct origin in statistics.

Dwork, McSherry, Nissim, & Smith (2006) is generally regarded as the first paper to formally introduce differential privacy. Its development was due, in part, to the *database reconstruction theorem* published by Dinur & Nissim (2003), which showed that most data publication mechanisms are blatantly non-private in a well-defined sense. The database reconstruction theorem has recently been shown to have very practical consequences for the statistical disclosure protections in place at the Census Bureau. The concepts of *k-anonymity* (Sweeney, 2002) and *l-diversity* (Ashwin Machanavajjhala, Kifer, Gehrke, & Venkitasubramaniam, 2007) are important antecedents that bridge the formal privacy and SDL literatures.

In assessing formal privacy as a framework for modeling data publication, it is natural to consider the optimal, or maximal amount of data accuracy that can be provided while maintaining privacy. Gupta, Roth, & Ullman (2012) establish a mechanism that is universally optimal for a broad class of data users, suggesting that technical efficiency could be guaranteed in private data publication without the need to learn about the preferences or side information of data consumers. However, Brenner & Nissim (2014) showed that their result is not generalizable to broader types of data publication. Nissim, Orlandi, & Smorodinsky (2012) provide a clear and instructive illustration of how individual preferences for privacy can be modeled in mechanism design problems.

Several papers are more directly relevant to understanding how privacy affects the work of statistical agencies. Cummings, Echenique, & Wierman (2014) argue that privacy concerns can affect the way people report data, and show how, if properly designed, privacy protection may mitigate misreporting. While there are vast number of papers on the implementation of differentially private publication algorithms, a few are particularly relevant to how statistical agencies operate. Hardt, Ligett, & McSherry (2012) and Hardt & Rothblum (2010) provide the methods and theory for publication through online query systems. One problem with these methods is that their implementation depends on the underlying data. By contrast, C. Li, Miklau, Hay, McGregor, & Rastogi (2015) introduce the Matrix Mechanism, which is data-independent, but also can provide high accuracy for reasonable levels of privacy. This is one of the methods under development for use with the 2020 Decennial Census. Other formal privacy systems currently in use at Census are documented in A. Machanavajjhala, Kifer, Abowd, Gehrke, & Vilhuber (2008) and Haney et al. (2017).

Finally, so-called "privacy semantics" are mappings between mathematical definitions of privacy and plain language. These are really important for practitioners because there is usually a gap between how laypeople think about privacy and how it is defined in the CS literature. By way of introduction, we recommend He, Machanavajjhala, & Ding (2014), Jorgensen, Yu, & Cormode (2015).

4 Policy and Official Statistics

In January 2017, the Committee on National Statistics released a special panel report focused on developing innovations in the U.S. statistical system focused, in part, on preserving privacy (National Academies of Sciences, Engineering, and Medicine, 2017). Their report is essential reading to understand the governing principles and practical needs of the statistical system, particularly as it relates to privacy modernization. For a more applied perspective, Schmutte & Vilhuber (2017) report the proceedings of an ad hoc workshop on practical privacy held at the Census Bureau. That workshop gathered together academic privacy researchers and Census domain experts to help design formal privacy systems for key data products. In such meetings, it is necessary to make sure people are speaking the same language. Prewitt (2011) describes the specific meanings of the terms "privacy" and "confidentiality" as they have historically been used at the Census Bureau.

Manski (2015) offers a framework for thinking about total error in official statistics, which refers to the various ways measured quantities may differ from the concepts of interest, including measurement error, design error, and sampling error. From this perspective, privacy protection is yet another source of error in any statistical system. Maintaining the public trust is a key factor motivating the interest of statistical agencies in privacy protection. The less people trust the system, the less likely they respond accurately, or at all. Childs, King, & Fobia (2015) discuss recent statistics on trust in official statistics and their implications for data collection. Finally, Haney et al. (2017) and Holan, Toth, Ferreira, & Karr (2010) are good examples of the sorts of implementation details one may encounter when applying statistical privacy protections in public data.

5 Statistical Disclosure Limitation

Within most national statistical systems, the primary approach to protecting respondent privacy has been *statistical disclosure limitation* or SDL. Anderson & Seltzer (2007) describes the history of threats to confidentiality in the U.S. statistical system prior to 1965. Fellegi (1972) initiated the statistical analysis of data confidentiality. Dalenius (1977) recognized that statistical agencies would need to do more than just protect against direct disclosures, and thus warned against what he called inferential disclosure. His idea was formalized by Duncan & Lambert (1986), and provides the ultimate rationale for formal privacy in national statistics.

J. M. Abowd & Schmutte (2015) review the SDL methods currently in use and discuss their application to economic data. They argue that the analysis of SDL-laden data is inherently compromised because the details of the SDL protections cannot be disclosed. If they cannot be disclosed, their consequences for inference are unknowable, and, as they show, potentially large. Garfinkel (2015) discusses techniques for de-identifying data and the many ways in which modern computing tools and a data-rich environment may render effective de-identification impossible. Finally, Harris-Kojetin et al. (2005) provides the most comprehensive review of SDL methods currently in use across the U.S. statistical system.

6 Economics of Privacy

There is a large and robust literature on privacy in economics. That literature is generally focused on the value to individuals of being able to conceal private information, like a health condition, from a firm or prospective employer. The challenge to the firm is to design mechanisms, like pricing strategies, that encourage people to disclose private information. For an overview of ideas in this literature, we recommend reading Stigler (1980), Posner (1981), and Hirshleifer (1980), which appeared in an early symposium. Varian (2002) and Acquisti, Taylor, & Wagman (2016) both provide comprehensive surveys at different points in the development of this literature.

Very few papers tie the economics of privacy directly to official statistics. Campbell, Goldfarb, & Tucker (2015) discuss the consequences for firm profits and individual welfare of data privacy restrictions in California, which prevent firms from sharing certain types of mortgage data. Goldfarb & Tucker (2012) discuss shifts in privacy attitudes and their implications for firms. Hsu et al. (2014), address the question of optimal privacy protection from a very similar perspective to J. M. Abowd & Schmutte (2019). Finally, Ohm (2010) surveys the economic implications of contemporary threats to data privacy from a legal perspective.

7 Value of Privacy and Data Accuracy

One key challenge for implementing formal privacy systems lies in choosing the amount, or type, of privacy to provide. Answering this question requires some way to understand the individual and social value of privacy. Ghosh & Roth (2015) and C. Li, Li, Miklau, & Suciu (2014) both model mechanisms for pricing private data under the assumption that individuals are only willing to disclose such information if they are paid.

Part of the social value of privacy arises from its relationship to scientific integrity. While the law of information recovery suggests that improved privacy must come at the cost of increased error in published statistics, these effects might be mitigated through two distinct channels. First, people are more truthful in surveys if they believe their data is not at risk, as Couper, Singer, Conrad, & Groves (2008) illustrate. Second, work in computer science (Dwork et al., 2015) and statistics (Cummings, Ligett, Nissim, Roth, & Wu, 2016) suggests another somewhat surprising benefit of differential privacy: protection against overfitting. A complete accounting of the costs and benefits of formal privacy systems should take these channels into account.

It is equally necessary to develop a more robust understanding of why data is valuable in the first place, the overall social cost of increasing error in public statistics. This seems to be an area in which very little comprehensive theoretical or empirical research has been done. We nevertheless recommend what seem to be good starting points.

On the theoretical side, economists studying privacy have also developed models of the value of data to firms. In these models, firms benefit from being able to tailor prices based on individual demand (C. R. Taylor, 2004), or from being able to market more effectively (Varian, 1998). More recently, a theoretical literature on information design has begun to consider more effective ways to manage markets for consumer information, see Bergemann, Bonatti, & Smolin (2018) and Pomatto, Strack, & Tamuz (2018). The recent literature is related to Bruce D. Spencer (1985), who developed a decision-theoretic framework for modeling optimal data quality.

On the empirical side, a handful of interesting use cases suggest techniques for uncovering the value of data. For example, Card, Mas, Moretti, & Saez (2012) and Perez-Truglia (2016) show how workers respond to pay transparency policies, which give them new information about co-worker salaries. Bruce David Spencer & Seeskin (2015) use a calibration exercise to study the costs, measured in misallocated congressional seats, of reduced accuracy in population census data.

8 References

13 U.S. Code. (1954). *USC: Title 13 - Census Act*. Retrieved from https://www.law.cornell.edu/uscode/pdf/lii_usc_TI_13.pdf

Abowd, J. M. (2016). Why statistical agencies need to take privacy-loss budgets seriously, and what it means when they do. *The 13th Biennial Federal Committee on Statistical Methodology (FCSM) Policy Conference*. Retrieved from https://digitalcommons.ilr.cornell.edu/ldi/32/

Abowd, J. M. (2017). How will statistical agencies operate when all data are private? *Journal of Privacy and Confidentiality*, *7*(3). https://doi.org/10.29012/jpc.v7i3.404

Abowd, J. M., & Schmutte, I. M. (2015). Economic analysis and statistical disclosure limitation. *Brookings Papers on Economic Activity*, 221–267. https://doi.org/10.1353/eca.2016.0004

Abowd, J. M., & Schmutte, I. M. (2019). An economic analysis of privacy protection and statistical accuracy as social choices. *American Economic Review*, *109*(1), 171–202. https://doi.org/10.1257/aer.20170627

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442

Anderson, M., & Seltzer, W. (2007). Challenges to the confidentiality of US federal statistics, 1910-1965. *Journal of Official Statistics*, *23*(1), 1. Retrieved from https://www.scb.se/contentassets/ff271eeeca694f47ae99b942de61df83/challenges-to-the-confidentiality-of-u.s.-federal-statistics-1910-1965.pdf

Bergemann, D., Bonatti, A., & Smolin, A. (2018). The design and price of information. *American Economic Review*, *108*(1), 1–48. https://doi.org/10.1257/aer.20161079

Brenner, H., & Nissim, K. (2014). Impossibility of differentially private universally optimal mechanisms. *SIAM Journal on Computing*, *43*(5), 1513–1540. https://doi.org/10.1137/110846671

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy regulation and market structure. *Journal of Economics & Management Strategy*, *24*(1), 47–73. https://doi.org/10.1111/jems.12079

Card, D., Mas, A., Moretti, E., & Saez, E. (2012). Inequality at work: The effect of peer salaries on job satisfaction. *American Economic Review*, *102*(6), 2981–3003. https://doi.org/10.1257/aer.102.6.2981

Childs, J. H., King, R., & Fobia, A. (2015). Confidence in U.S. federal statistical agencies. *Survey Practice*, *8*(5). https://doi.org/10.29115/sp-2015-0024

Couper, M. P., Singer, E., Conrad, F. G., & Groves, R. M. (2008). Risk of disclosure, perceptions of risk, and concerns about privacy and confidentiality as factors in survey participation. *Journal of Official Statistics*, *24*(2), 255. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3096944/

Cummings, R., Echenique, F., & Wierman, A. (2014). The empirical implications of privacy-aware choice. *CoRR*, *abs/1401.0336*. Retrieved from http://arxiv.org/abs/1401.0336

Cummings, R., Ligett, K., Nissim, K., Roth, A., & Wu, Z. S. (2016). Adaptive learning with robust generalization guarantees. *CoRR*, *abs/1602.07726*. Retrieved from http://arxiv.org/abs/1602.07726

Dalenius, T. (1977). Towards a methodology for statistical disclosure control. *Statistik Tidskrift*, *15*, 429–444. https://doi.org/10.1145/320613.320616

Dinur, I., & Nissim, K. (2003). Revealing information while preserving privacy. *Proceedings of the Twenty-second ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, 202–210. https://doi.org/10.1145/773153.773173

Duncan, G., & Lambert, D. (1986). Disclosure-limited data dissemination. *Journal of the American Statistical Association*, *81*(393), 10–18. https://doi.org/10.1080/01621459.1986.10478229

Dwork, C., & Roth, A. (2014). The Algorithmic Foundations of Differential Privacy. *Foundations and Trends in Theoretical Computer Science*, *9*(3-4), 211–407. https://doi.org/10.1561/0400000042

Dwork, C., Feldman, V., Hardt, M., Pitassi, T., Reingold, O., & Roth, A. (2015). Generalization in adaptive data analysis and holdout reuse. In C. Cortes, N. D. Lawrence, D. D. Lee, M. Sugiyama, & R. Garnett (Eds.), *Advances in neural information processing systems 28* (pp. 2341–2349). Retrieved from http://papers.nips.cc/paper/5993-generalization-in-adaptive-data-analysis-and-holdout-reuse.pdf

Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating Noise to Sensitivity in Private Data Analysis. *Proceedings of the Third conference on Theory of Cryptography*, 265–284. https://doi.org/10.1007/11681878_14

Fellegi, I. P. (1972). On the question of statistical confidentiality. *Journal of the American Statistical Association*, *67*(337), 7–18. https://doi.org/10.2307/2284695

Garfinkel, S. (2015). *De-Identification of personal information* (Internal Report No. 8053). https://doi.org/10.6028/nist.ir.8053

Ghosh, A., & Roth, A. (2015). Selling privacy at auction. *Games and Economic Behavior*, *91*, 334–346. https://doi.org/10.1016/j.geb.2013.06.013

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. *American Economic Review*, *102*(3), 349–353. https://doi.org/10.1257/aer.102.3.349

Goroff, D. L. (2015). Balancing privacy versus accuracy in research protocols. *Science*, *347*(6221), 479–480. https://doi.org/10.1126/science.aaa3483

Gupta, A., Roth, A., & Ullman, J. (2012). Iterative constructions and private data release. *Proceedings of the 9th International Conference on Theory of Cryptography*, 339–356. https://doi.org/10.1007/978-3-642-28914-9_19

H.R.4174. (2018). *Confidential Information Protection and Statistical Efficency Act.* Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/4174

Haney, S., Machanavajjhala, A., Abowd, J. M., Graham, M., Kutzbach, M., & Vilhuber, L. (2017). Utility cost of formal privacy for releasing national employer-employee statistics. In *SIGMOD '17. Proceedings of the 2017 International Conference on Management of Data.* https://doi.org/10.1145/3035918.3035940

Hardt, M., & Rothblum, G. N. (2010). A multiplicative weights mechanism for privacy-preserving data analysis. *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, 61–70. https://doi.org/10.1109/FOCS.2010.85

Hardt, M., Ligett, K., & McSherry, F. (2012). A Simple and Practical Algorithm for Differentially Private Data Release. In F. Pereira, C. Burges, L. Bottou, & K. Weinberger (Eds.), *Advances in neu-*

ral information processing systems 25 (pp. 2339–2347). Retrieved from http://papers.nips.cc/paper/4548-a-simple-and-practical-algorithm-for-differentially-private-data-release.pdf

Harris-Kojetin, B. A., Alvey, W. L., Carlson, L., Cohen, S. B., Cohen, S. H., Cox, L. H., … Groves, R. (2005). *Statistical policy working paper 22: Report on statistical disclosure limitation methodology* [Research Report]. Retrieved from U.S. Federal Committee on Statistical Methodology website: https://nces.ed.gov/FCSM/pdf/spwp22.pdf

Harvard University Privacy Tools Project. (2019). *Homepage.* Retrieved from https://privacytools.seas.harvard.edu/

He, X., Machanavajjhala, A., & Ding, B. (2014). Blowfish privacy: Tuning privacy-utility trade-offs using policies. In *Proceedings of the acm sigmod international conference on management of data* (pp. 1447–1458). https://doi.org/10.1145/2588555.2588581

Heffetz, O., & Ligett, K. (2014). Privacy and data-based research. *Journal of Economic Perspectives*, *28*(2), 75–98. https://doi.org/10.1257/jep.28.2.75

Hirshleifer, J. (1980). Privacy: Its origin, function, and future. *The Journal of Legal Studies*, 649–664. https://doi.org/10.1086/467659

Holan, S. H., Toth, D., Ferreira, M. A. R., & Karr, A. F. (2010). Bayesian multiscale multiple imputation with implications for data confidentiality. *Journal of the American Statistical Association*, *105*(490), 564–577. https://doi.org/10.1198/jasa.2009.ap08629

Hsu, J., Gaboardi, M., Haeberlen, A., Khanna, S., Narayan, A., Pierce, B. C., & Roth, A. (2014). Differential privacy: An economic method for choosing epsilon. *2014 IEEE 27th Computer Security Foundations Symposium*, 398–410. https://doi.org/10.1109/CSF.2014.35

Jones, C. (2017). *Nonconfidential memorandum on Census Bureau privacy breaches.* Retrieved from http://doi.org/10.5281/zenodo.1345775

Jorgensen, Z., Yu, T., & Cormode, G. (2015). Conservative or liberal? Personalized differential privacy. *2015 IEEE 31st International Conference on Data Engineering*, 1023–1034. https://doi.org/10.1109/ICDE.2015.7113353

Li, C., Li, D. Y., Miklau, G., & Suciu, D. A. N. (2014). A theory of pricing private data. *ACM Transactions on Database Systems*, *39*(4), 34:1–34:27. https://doi.org/10.1145/2448496.2448502

Li, C., Miklau, G., Hay, M., McGregor, A., & Rastogi, V. (2015). The matrix mechanism: Optimizing linear counting queries under differential privacy. *The VLDB Journal*, *24*(6), 757–781. https://doi.org/10.1007/s00778-015-0398-x

Machanavajjhala, A., Kifer, D., Abowd, J., Gehrke, J., & Vilhuber, L. (2008). Privacy: Theory meets practice on the map. *Proceedings of the 2008 ieee 24th international conference on data engineering*, 277–286. https://doi.org/10.1109/ICDE.2008.4497436

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). L-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data*, *1*(1). https://doi.org/10.1145/1217299.1217302

Manski, C. F. (2015). Communicating uncertainty in official economic statistics: An appraisal fifty years after morgenstern. *Journal of Economic Literature*, *53*(3), 631–653. https://doi.org/10.1257/jel.53.3.631

National Academies of Sciences, Engineering, and Medicine. (2017). *Innovations in federal statistics: Combining data sources while protecting privacy.* https://doi.org/10.17226/24652

Nissim, K., Orlandi, C., & Smorodinsky, R. (2012). Privacy-aware mechanism design. *Proceedings of the 13th acm conference on electronic commerce*, 774–789. https://doi.org/10.1145/2229012.2229073

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA*

Law Review, *57*, 1701.

Perez-Truglia, R. (2016). The effects of income transparency on well-being: Evidence from a natural experiment. *SSRN*. https://doi.org/10.2139/ssrn.2657808

Pomatto, L., Strack, P., & Tamuz, O. (2018). *The cost of information*. arXiv.

Posner, R. A. (1981). The economics of privacy. *The American Economic Review*, 405–409.

Prewitt, K. (2011). Why It Matters to Distinguish Between Privacy & Confidentiality. *Journal of Privacy and Confidentiality*, *3*(2), 41–47. https://doi.org/10.29012/jpc.v3i2.600

Schmutte, I. M., & Vilhuber, L. (Eds.). (2017). *Proceedings from the 2016 NSF-Sloan Workshop on Practical Privacy*. Retrieved from https://digitalcommons.ilr.cornell.edu/ldi/33/

Spencer, B. D. (1985). Optimal data quality. *Journal of the American Statistical Association*, *80*(391), 564–573. https://doi.org/10.1080/01621459.1985.10478155

Spencer, B. D., & Seeskin, Z. H. (2015). Effects of Census accuracy on apportionment of Congress and allocations of federal funds. *JSM Proceedings, Government Statistics Section*, 3061–3075. Retrieved from https://www.ipr.northwestern.edu/publications/papers/2015/ipr-wp-15-05.html

Stigler, G. J. (1980). An introduction to privacy in economics and politics. *Journal of Legal Studies*, *9*(4), 623–644. https://doi.org/10.2307/724174

Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(5), 571–588. https://doi.org/10.1142/s021848850200165x

Taylor, C. R. (2004). Consumer privacy and the market for customer information. *The RAND Journal of Economics*, *35*(4), 631–650. https://doi.org/10.2307/1593765

Varian, H. R. (1998). *Markets for Information Goods* (pp. 1–19) [Mimeo]. Retrieved from UC Berkeley School of Information website: http://people.ischool.berkeley.edu/~hal/Papers/japan/index.html

Varian, H. R. (2002). Economic aspects of personal privacy. In W. H. Lehr & L. M. Pupillo (Eds.), *Cyber policy and economics in an internet age* (pp. 127–137). https://doi.org/10.1007/978-1-4757-3575-8_9

Wood, A., Altman, M., Bembenek, A., Bun, M., Gaboardi, M., Honaker, J., … Vadhan, S. (2018). Differential Privacy: A Primer for a Non-Technical Audience. *Vanderbilt Journal of Entertainment and Technology Law*, *21*(1). Retrieved from http://www.jetlaw.org/journal-archives/volume-21/volume-21-issue-1/differential-privacy-a-primer-for-a-non-technical-audience/