Volume Title: The Economics of Artificial Intelligence: An Agenda

Volume Authors/Editors: Ajay Agrawal, Joshua Gans, and Avi Goldfarb, editors

Volume Publisher: University of Chicago Press

Volume ISBNs: 978-0-226-61333-8 (cloth); 978-0-226-61347-5 (electronic)

Volume URL: http://www.nber.org/books/agra-1

Conference Date: September 13–14, 2017

Publication Date: May 2019

Chapter Title: Privacy, Algorithms, and Artificial Intelligence

Chapter Author(s): Catherine Tucker

Chapter URL: http://www.nber.org/chapters/c14011

Chapter pages in book: (p. 423 – 437)

17

Privacy, Algorithms, and Artificial Intelligence

Catherine Tucker

Imagine the following scenario. You are late for a hospital appointment and searching frantically for a parking spot. You know that you often forget where you parked your car, so you use an app you downloaded called "Find my Car." The app takes a photo of your car and then geocodes the photo, enabling you to easily find the right location when you come to retrieve your car. The app accurately predicts when it should provide a prompt. This all sounds very useful. However, this example illustrates a variety of privacy concerns in a world of artificial intelligence.

1. Data Persistence: This data, once created, may potentially persist longer than the human that created it, given the low costs of storing such data.
2. Data Repurposing: It is not clear how such data could be used in the future. Once created, such data can be indefinitely repurposed. For example, in a decade's time parking habits may be part of the data used by health insurance companies to allocate an individual to a risk premium.
3. Data Spillovers: There are potential spillovers for others who did not take the photo. The photo may record other people and they may be identifiable through facial recognition, or incidentally captured cars may be identifiable through license plate databases. These other people did not choose to create the data, but my choice to create data may have spillovers for them in the future.

Catherine Tucker is the Sloan Distinguished Professor of Management Science at MIT Sloan School of Management and a research associate of the National Bureau of Economic Research.

For acknowledgments, sources of research support, and disclosure of the author's material financial relationships, if any, please see http://www.nber.org/chapters/c14011.ack.

This article will discuss these concerns in detail, after considering how the theory of the economics of privacy relates to artificial intelligence (AI).

17.1 The Theory of Privacy in Economics and Artificial Intelligence

17.1.1 Current Models of Economics and Privacy and Their Flaws

The economics of privacy has long being plagued by a lack of clarity about how to model privacy over data. Most theoretical economic models model privacy as an intermediate good (Varian 1996; Farrell 2012). This implies that an individual desire for data privacy will depend on how they anticipate that data's effect on future economic outcomes. If, for example, this data leads a firm to charge higher prices based on the behavior they observe in the data, a consumer may desire privacy. If a datum may lead a firm to intrude on their time, then again a consumer may desire privacy.

However, this contrasts with, or at the very least has a different emphasis on, how many policymakers and even consumers think about privacy policy and choice.

First, much of the policy debate involves whether or not consumers are capable of making the right choice surrounding the decision to provide data, and whether "notice and consent" provides sufficient information to consumers so they make the right choice. Work such as McDonald and Cranor (2008) emphasizes that even ten years ago it was unrealistic to think that consumers would have time to properly inform themselves about how their data may be used, as reading through privacy policies would take an estimated 244 hours each year. Since that study, the amount of devices (thermostats, smart phones, apps, cars) collecting data has increased dramatically, suggesting that it is, if anything, more implausible now that a consumer has the time to actually understand the choice they are making in each of these instances.

Relatedly, even if customers are assumed to have been adequately informed, a new "behavioral" literature on privacy shows that well-documented effects from behavioral economics, such as the endowment effect or "anchoring," may also distort the ways customers make decisions surrounding their data (Acquisti, Taylor, and Wagman 2016). Such distortions may allow for policy interventions of the "nudge" type to allow consumers to make better decisions (Acquisti 2010).

Third, this theory presupposes that customers will only desire privacy if their data is actually used for something, rather than experiencing distaste at the idea of their data being collected. Indeed, in some of the earliest work on privacy in the internet era, Varian (1996) states, "I don't really care if someone has my telephone number as long as they don't call me during dinner and try to sell me insurance. Similarly, I don't care if someone has my address, as long as they don't send me lots of official-looking letters offering to refinance my house or sell me mortgage insurance."

However, there is evidence to suggest that people do care about the mere fact of collection of their data to the extent of changing their behavior, even if the chance of their suffering meaningfully adverse consequences from that collection is very small. Empirical analysis of people's reactions to the knowledge that their search queries (Marthews and Tucker 2014) had been collected by the US National Security Agency (NSA), shows a significant shift in behavior even when that data was not going to be used by the government to identify terrorists, as it was simply personally embarrassing. Legally speaking, the Fourth Amendment of the US Constitution covers the "unreasonable seizure" as well as the "unreasonable search" of people's "papers and effects," suggesting that governments, and firms acting on government's behalf, cannot entirely ignore seizure of data and focus only on whether a search is reasonable. Consequently, a growing consumer market has emerged for "data-light" and "end-to-end encrypted" communications and software solutions, where the firm collects much less or no data about their consumers' activities on their platform. These kinds of concern suggest that the fact of data collection may matter as well as how the data is used.

Last, often economic theory assumes that while customers desire firms to have information that allows them to better match their horizontally differentiated preferences, they do not desire firms to have information that might inform their willingness to pay (Varian 1996). However, this idea that personalization in a horizontal sense may be sought by customers goes against popular reports of consumers finding personalization repugnant or creepy (Lambrecht and Tucker 2013). Instead, it appears that personalization of products using horizontally differentiated taste information is only acceptable or successful if accompanied by a sense of control or ownership over the data used, even where such control is ultimately illusory (Tucker 2014; Athey, Catalini, and Tucker 2017).

17.1.2 Artificial Intelligence and Privacy

Like "privacy," artificial intelligence is often used loosely to mean many things. This article follows (Agrawal, Gans, and Goldfarb 2016) and focuses on AI as being associated with reduced costs of prediction. The obvious effect that this will have on the traditional model of privacy is that more types of data will be used to predict a wider variety of economic objectives.

Again, the desire (or lack of desire) for privacy will be a function of an individual's anticipation of the consequences of their data being used in a predictive algorithm. If they anticipate that they will face worse economic outcomes if the AI uses their data, they may desire to restrict their data sharing or creating behavior.

It may be that the simple dislike or distaste for data collection will transfer to the use of automated predictive algorithms to process their data. The creepiness that leads to a desire for privacy that is attached to the use of data would be transferred to algorithms. Indeed, there is some evidence of a similar behavioral process where some customers only accept algorithmic prediction if it is accompanied by a sense of control (Dietvorst, Simmons, and Massey 2016).

In this way, the question of AI algorithms seems simply a continuation of the tension that has plagued earlier work in the economics of privacy. So, a natural question is whether AI presents new or different problems. This article argues that many of the questions of AI and privacy choices will constrain the ability of customers in our traditional model of privacy to make choices regarding the sharing of their data. I emphasize three themes that I think may distort this process in important and economically interesting ways.

17.2 Data Persistence, AI, and Privacy

Data persistence refers to the fact that once digital data is created, it is difficult to delete completely. This is true from a technical perspective (Adee 2015). Unlike analog records, which can be destroyed with reasonable ease, the intentional deletion of digital data requires resources, time, and care.

17.2.1 Unlike in Previous Eras, Data Created Now Is Likely to Persist

Cost constraints that used to mean that only the largest firms could afford to store extensive data, and even then for a limited time, have essentially disappeared.

Large shifts in the data-supply infrastructure have rendered the tools for gathering and analyzing large swaths of digital data commonplace. Cloud-based resources such as Amazon, Microsoft, and Rackspace make these tools not dependent on scale,[1] and storage costs for data continue to fall, so that some speculate they may eventually approach zero.[2] This allows ever-smaller firms to have access to powerful and inexpensive computing resources. This decrease in costs suggests that data may be stored indefinitely and can be used in predictive exercises should it be thought of as a useful predictor.

The chief resource constraint on the deployment of big data solutions is a lack of human beings with the data-science skills to draw appropriate conclusions from analysis of large data sets (Lambrecht and Tucker 2017). As time and skills evolve, this constraint may become less pressing.

Digital persistence may be concerning from a privacy point of view because privacy preferences may change over time. The privacy preference

[1] http://betanews.com/2014/06/27/comparing-the-top-three-cloud-storage-providers/.

[2] http://www.enterprisestorageforum.com/storage-management/can-cloud-storage-costs-fall-to-zero-1.html.

that an individual may have felt when they created the data may be inconsistent with the privacy preference of their older self. This is something we documented in Goldfarb and Tucker (2012). We showed that while younger people tended to be more open with data, as they grew older their preference for withholding data grew. This was a stable effect that persisted across cohorts. It is not the case that young people today are unusually casual about data; all generations when younger are more casual about data, but this pattern was simply less visible previously because social media, and other ways of sharing and creating potentially embarrassing data, did not yet exist.

This implies that one concern regarding AI and privacy is that it may use data that was created a long time in the past, which in retrospect the individual regrets creating.

Data that was created at $t = 0$ may have seemed innocuous at the time, and in isolation may still be innocuous at $t = t + 1$, but increased computing power may be able to derive much more invasive conclusions from aggregations of otherwise innocuous data at $t + 1$ relative to t. Second, there is a whole variety of data generated on individuals that individuals do not necessarily consciously choose to create. This not only includes incidental collection of the data such as being photographed by another party, but also data generated by the increased passive surveillance of public spaces, and the use of cellphone technology without full appreciation of how much data about an individual and location it discloses to third parties, including the government.

Though there has been substantial work in bringing in the insights of behavioral economics into the study of the economics of privacy, there has been less work on time-preference consistency, despite the fact that it is one of the oldest and most studied (Strotz 1955; Rubinstein 2006) phenomena in behavioral economics. Introducing the potential for myopia or hyperbolic discounting into the way we model privacy choices over the creation of data seems, therefore, an important step. Even if the economist concerned rejects behavioral economics or myopia as an acceptable solution, at the very least it is useful to emphasize that privacy choices should be modeled not as something where the time between the creation of the data and the use of the data is trivial, but instead is more acceptably modeled as a decision that may be played out over an extended amount of time.

17.2.2 How Long Will Data's Predictive Power Persist?

If we assume that any data created will probably persist, given low storage costs, it may be that the more important question for understanding the dynamics of privacy is the question of how long data's predictive power persists.

It seems reasonable to think that much of the data created today does not have much predictive power tomorrow. This is something we investigated in

Chiou and Tucker (2014) where we showed that the length of the data retention period that search engines were restricted to by the European Union (EU) did not appear to affect the success of their algorithm at generating useful search results. This is where the success of a search result was measured by whether or not the user felt compelled to search again. This may make sense in the world of search engines where many searches are either unique or focused on new events. On August 31, 2017, for example, the top trending search on Google was "Hurricane Harvey," something that could not have been predicted on the basis of search behavior from more than a few weeks prior.[3]

However, there are some forms of data where it is reasonable to think that their predictive power will persist almost indefinitely. The most important example of this is the creation of genetic digital data. As Miller and Tucker (2017) point out, companies such as 23andme.com are creating large repositories of genetic data spanning more than 1.2 million people. As pointed out by Miller and Tucker (2017), genetic data has the unusual quality that it does not change over time.

While the internet browsing behavior of a twenty-year-old may not prove to be good for predicting their browsing behavior at age forty, the genetic data of a twenty-year-old will almost perfectly predict the genetic data of that person when they turn forty.[4]

17.3 Data Repurposing, AI, and Privacy

The lengthy time frame that digital persistence of data implies increases uncertainty surrounding how the data will be used. This is because once created, a piece of data can be reused an infinite number of times. As prediction costs are lower, this generally expands the number of circumstances and occasions where data may be used. If an individual is unable to reasonably anticipate how their data may be repurposed or what the data may predict in this repurposed setting, modeling their choices over the creation of their data becomes more difficult and problematic than in our current very deterministic models, which assume certainty over how data will be used.

17.3.1 Unanticipated Correlations

There may be correlations in behavior across users that may not be anticipated when data is created, and it is in these kinds of spillovers that the largest potential consequences for privacy of AI may be found.

One famous example of this is that someone liking (or disliking) curly fries on Facebook would have been unable to reasonably anticipate it would be

[3] https://trends.google.com/trends/.

[4] As discussed in articles such as http://www.nature.com/news/2008/080624/full/news.2008.913.html, DNA does change somewhat over time, but that change is itself somewhat predictable.

predictive of intelligence (Kosinski, Stillwell, and Graepel 2013) and therefore potentially used as a screening device by algorithms aiming to identify desirable employees or students.[5]

17.3.2 Unanticipated Distortions in Correlations

In these cases, an algorithm could potentially make a projection based on a correlation in the data, using data that was created for a different purpose. The consequences for models of economics of privacy are that they assume a singular use of data, rather than allowing for the potential of reuse in unpredictable contexts.

However, even supposing that individuals were able to reasonably anticipate the repurposing of their data, there are incremental challenges with thinking about their ability to project distortions that might come about as a result of the repurposing of their data.

The potential for distortions based on correlations in data is something we investigate in new research.[6]

In Miller and Tucker (2018) we document the distribution of advertising by an advertising algorithm that attempts to predict a person's ethnic affinity from their data online. We ran multiple parallel ad campaigns targeted at African American, Asian American, and Hispanic ethnic affinities. We also ran an additional campaign targeted at those judged to not have any of these three ethnic affinities. These campaigns highlighted a federal program designed to enhance pathways to a federal job via internships and career guidance.[7] We ran this ad for a week and collected data on how many people the ad was shown to in each county. We found that relative to what would be predicted by the actual demographic makeup of that county given the census data, the ad algorithm tended to predict that more African American people are in states where there is a historical record of discrimination against African Americans. This pattern is true for states that allowed slavery at the time of the American Civil War, and also true for states that restricted the ability of African Americans to vote in the twentieth century. In such states, it was only the presence of African Americans that was over predicted, not people with Hispanic or Asian American backgrounds.

We show that this cannot be explained by the algorithm responding to behavioral data in these states, as there was no difference in click-through patterns across different campaigns across states, with or without this history of discrimination.

[5] This study found that the best predictors of high intelligence include Thunderstorms, *The Colbert Report*, *Science*, and Curly Fries, whereas low intelligence was indicated by Sephora, I Love Being A Mom, Harley Davidson, and Lady Antebellum.

[6] This new research will be the focus of my presentation at the NBER meetings.

[7] For details of the program, see https://www.usajobs.gov/Help/working-in-government/unique-hiring-paths/students/.

We discuss how this can be explained by four facts about how the algorithm operates:

1. The algorithm identifies a user as having a particular ethnic affinity based on their liking of cultural phenomena such as celebrities, movies, TV shows, and music.
2. People who have lower incomes are more likely to use social media to express interest in celebrities, movies, TV shows, and music.
3. People who have higher incomes are more likely to use social media to express their thoughts about the politics and the news.[8]
4. Research in economics has suggested that African Americans are more likely to have lower incomes in states that have exhibited historic patterns of discrimination (Sokoloff and Engerman 2000; Bertocchi and Dimico 2014).

The empirical regularity that an algorithm predicting race is more likely to predict someone is black in geographies that have historic patterns of discrimination matters because it highlights the potential for historical persistence in algorithmic behavior. It suggests that dynamic consequences of earlier history may affect how artificial intelligence makes predictions. When that earlier history is repugnant, it is even more concerning. In this particular case the issue is using a particular piece of data to predict a trait when the generation of that data is endogenous.

This emphasizes that privacy policy in a world of predictive algorithms is more complex than in a straightforward world where individuals make binary decisions about their data. In our example, it would seem problematic to bar low-income individuals from expressing their identities via their affinity with musical or visual arts. However, their doing so could likely lead to a prediction that they belong to a particular ethnic group. They may not be aware ex ante of the risk that disclosing a musical preference may cause Facebook to infer an ethnic affinity and advertise to them on that basis.

17.3.3 Unanticipated Consequences of Unanticipated Repurposing

In most economic models, a consumer's prospective desire for privacy in the data depends here on the consumer being able to accurately forecast the uses to which the data is put. One problem with data privacy is that AI/algorithmic use of existing data sets may be reaching a point where data can be used and recombined in ways that people creating that data in, say, 2000 or 2005, could not reasonably have foreseen or incorporated into their decision-making at the time.

Again, this brings up legal concerns where an aggregation, or mosaic, of data on an individual is held to be sharply more intrusive than each datum considered in isolation. In *United States v. Jones* (2012), Justice Sotomayor wrote in a well-known concurring opinion, "It may be necessary to

[8] One of the best predictors of high income on social media is a liking of Dan Rather.

reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties [. . .]. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." Artificial intelligence systems have shown themselves as able to develop very detailed pictures of individuals' tastes, activities, and opinions based on analysis of aggregated information on our now digitally intermediated mundane tasks. Part of the risk in a mosaic approach for firms is that data previously considered not personally identifiable or personally sensitive—such as ZIP Code, gender, or age to within ten years—when aggregated and analyzed by today's algorithms, may suffice to identify you as an individual.

This general level of uncertainty surrounding the future use of data, coupled with certainty that it will be potentially useful to firms, affects the ability of a consumer to be able to clearly make a choice to create or share data. With large amounts of risk and uncertainty surrounding how private data may be used, this has implications for how an individual may process their preferences regarding privacy.

17.4 Data Spillovers, AI, and Privacy

In the United States, privacy has been defined as an individual right, specifically an individual's right to be left alone (Warren and Brandeis 1890) (in this specific case, from journalists with cameras).

Economists' attempts to devise a utility function that reflects privacy have reflected this individualistic view. A person has a preference for keeping information secret (or not) because of the potential consequences for their interaction with a firm. So far, their privacy models have not reflected the possibility that another person's preferences or behavior could have spillovers on this process.

17.5 Some Types of Data Used by Algorithms May Naturally Generate Spillovers

For example, in the case of genetics, the decision to create genetic data has immediate consequences for family members, since one individual's genetic data is significantly similar to the genetic data of their family members. This creates privacy spillovers for relatives of those who upload their genetic profile to 23andme. Data that predicts I may suffer from bad eyesight or macular degeneration later in life could be used to reasonably predict that those who are related to me by blood may also be more likely to share a similar risk profile.

Of course, one hopes that an individual would be capable of internalizing the potential externalities on family members of genetic data revelation, but it does not seem far-fetched to imagine situations of estrangement where such internalizing would not happen and there would be a clear externality.

Outside the realm of binary data, there are other kinds of data that by their nature may create spillovers. These include photo, video, and audio data taken in public places. Such data may be created for one purpose such as the result of a recreational desire to use video to capture a memory or to enhance security, but may potentially create data about other individuals whose voices or images are captured without them being aware that their data is being recorded. Traditionally, legal models of privacy have distinguished between the idea of a private realm where an individual has an expectation of privacy and a public realm where an individual can have no reasonable expectation of privacy. For example, in the Supreme Court case *California v. Greenwood* (1988), the court refused to accept that an individual had a reasonable expectation of privacy in garbage he had left on the curb.

However, in a world where people use mobile devices and photo capture extensively, facial recognition allows accurate identification of any individual while out in public, and individuals have difficulty avoiding such identifications. Encoded in the notion that we do not have a reasonable expectation of privacy in the public realm are two potential errors: that one's presence in a public space is usually transitory enough to not be recorded, and that the record of one's activities in the public space will not usually be recorded, parsed, and exploited for future use. Consequently, the advance of technology muddies the allocation of property rights over the creation of data. In particular, it is not clear how video footage of my behavior in public spaces, which can potentially accurately predict economically meaningful outcomes such as health outcomes, can be clearly dismissed as being a context where I had no expectation of privacy, or at least no right to control the creation of data. In any case, these new forms of data, due in some sense to the incidental nature of data creation seem to undermine the clear-cut assumption of easily definable property rights over the data that is integral to most economic models of privacy.

17.5.1 Algorithms Themselves Will Naturally Create Spillovers across Data

One of the major consequences of AI and its ability to automate prediction is that there may be spillovers between individuals and other economic agents. There may also be spillovers across a person's decision to keep some information secret, if such secrecy predicts other aspects of that individual's behavior that AI might be able to project from.

Research has documented algorithmic outcomes that appear to be discriminatory, and has argued that such outcomes may occur because the algorithm itself will learn to be biased on the basis of the behavioral data that feeds it (O'Neil 2017). Documented alleged algorithmic bias spans charging more to Asians for test-taking prep software[9] to black names being more likely to produce criminal record check ads (Sweeney 2013) to women being less likely to seeing ads for an executive coaching service (Datta, Tschantz, and Datta 2015).

Such data-based discrimination is often held to be a privacy issue (Custers et al. 2012). The argument is that it is abhorrent for a person's data to be used to discriminate against them—especially if they did not explicitly consent to its collection in the first place. However, though not often discussed in the legally orientated data-based discrimination literature, there are many links between the fears expressed for the potential of data-based discrimination and the earlier economics literature on statistical discrimination literature. In much the same way that some find it distasteful when an employer extrapolates from general data on fertility decisions and consequences among females to project similar expectations of fertility and behavior onto a female employee, an algorithm making similar extrapolations is equally distasteful. Such instances of statistical discrimination by algorithms may reflect spillovers of predictive power across individuals, which in turn may not be necessarily internalized by each individual.

However, as of yet there have been few attempts to try to understand why ad algorithms can produce apparently discriminatory outcomes, or whether the digital economy itself may play a role in the apparent discrimination. I argue that above and beyond the obvious similarity to the statistical discrimination literature in economics, sometimes apparent discrimination can be best understood as spillovers in algorithmic decision-making. This makes the issue of privacy not just one of the potential that an individual's data can be used to discriminate against them.

In Lambrecht and Tucker (forthcoming), we discuss a field study into apparent algorithmic bias. We use data from a field test of the display of an ad for jobs in the science, technology, engineering, and math fields (STEM). This ad was less likely to be shown to women. This appeared to be a result of an algorithmic outcome, as the advertiser had intended the ad to be gender neutral. We explore various ways that might explain why the algorithm acted in an apparently discriminatory way. An obvious set of explanations is ruled out. For example, it is not because the predictive algorithm has fewer women to show the ad to, and it is not the case that the predictive algorithm learns that women are less likely are to click the ad, since women are more likely to click on it—conditional on being shown the ad—than men. In other words, this is not simply statistical discrimination. We also show it is not that

[9] https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review. In this case, the alleged discrimination apparently stemmed from the fact that Asians are more likely to live in cities that have higher test prep prices.

the algorithm learned from local behavior that may historically have been biased against women. We use data from 190 countries and show that the effect we measure does not appear to be influenced by the status of women in that country. Instead, we present evidence that the algorithm is reacting to spillovers across advertisers. Women are a prized demographic among advertisers, both because they are often more profitable and because they control much of the household expenditure. Therefore, profit-maximizing firms pay more to show ads to female eyeballs than male eyeballs, especially in younger demographics. These spillovers across advertisers and the algorithms' attempts to cost-minimize given these spillovers explain the effect we measure. Women are less likely to see an intended gender-neutral ad due to crowding out effects.

To put it simply, our results are the result of these factors:

1. The ad algorithm is designed to minimize cost so that advertisers' advertising dollars will stretch further.
2. Other advertisers consider female eyeballs to be more desirable and deliver a higher return on investment and therefore are willing to pay more to have their ads shown to women than men.

Lambrecht and Tucker (forthcoming) explore apparent algorithmic bias, which is the consequence of clear economic spillovers between the value of a pair of eyeballs for one organization compared to another. Beyond ensuring that, for example, firms advertising for jobs are aware of the potential consequences, it is difficult to know what policy intervention is needed or the extent to which this should be thought of as a privacy issue rather than analyzed through the already established policy tools set up to address discrimination.

This kind of spillover, though, is another example of how in an interconnected economy, models of privacy that stipulate privacy as an exchange between a single firm and a single consumer may no longer be appropriate for a connected economy. Instead, the way any piece of data may be used by a single firm may itself be subject to spillovers from other entities in the economy, again in ways that may not be easily foreseen at the time of data creation.

17.6 Implications and Future Research Agenda

This chapter is a short introduction into the relationship between artificial intelligence and the economics of privacy. It has emphasized three themes: data persistence, data repurposing, and data spillovers. These three areas may present some new challenges for the traditional treatment of privacy within an individual's utility function as they suggest challenges for the ways we model how an individual may make choices about the creation of personal data that can later be used to inform an algorithm. At the highest level, this suggests that future work on privacy in economics may focus on the dynamics of privacy considerations amid data persistence and repurposing, and the spillovers that undermine the clarity of property rights over data, rather than the more traditional atomistic and static focus of our economic models of privacy.

17.6.1 Future Research Agenda

To conclude this chapter, I highlight specific research questions that fall under these three areas:

- Data Persistence

1. What causes consumers' privacy preferences to evolve over time? How stable are these preferences and for how long?
2. Are consumers able to correctly predict the evolution of their privacy preferences as they get older?
3. Would regulations designed to restrict the length of time that companies can store data be welfare enhancing or reducing?
4. What influences the persistence of the value of data over the long run? Are there some types of data that lose their value to algorithms quickly?

- Data Reuse

1. Do consumers appreciate the extent to which their data can be reused and are they able to predict what their data may be able to predict?
2. What kind of regulations restricting data reuse may be optimal?
3. Do approaches to data contracting based on the blockchain or other transaction cost-reducing technologies enable sufficiently broad contracts (and the establishment of property rights) over data?
4. Are there any categories of data where reuse by algorithms should be explicitly restricted?

- Data Spillovers

1. Are there any mechanisms (either theoretical or practical) that could be used to ensure that people internalized the consequences of their creation of data for others?
2. What is the best mechanism by which individuals may be able to assert their right to exclusion from some types of data that are being broadly collected (genetic data, visual data, surveillance data, etc.)?
3. Is there any evidence for the hypothesis of biased AI programmers, leading to biased AI algorithms? Would efforts to improve diversity in the technology community reduce the potential for bias?
4. How much more biased are algorithms that appear to engage in data-based discrimination than the counterfactual human process?

References

Acquisti, A. 2010. "From the Economics to the Behavioral Economics of Privacy: A Note." In *Ethics and Policy of Biometrics*, edited by A. Kumar and D. Zhang, 23–26. Lecture Notes in Computer Science, vol. 6005. Berlin: Springer.

Acquisti, A., C. R. Taylor, and L. Wagman. 2016. "The Economics of Privacy." *Journal of Economic Literature*, 52 (2): 442–92.

Adee, S. 2015. "Can Data Ever Be Deleted? *New Scientist* 227 (3032): 17.

Agrawal, A., J. Gans, and A. Goldfarb. 2016. "The Simple Economics of Machine Intelligence." *Harvard Business Review*, Nov. 17. https://hbr.org/2016/11/the-simple-economics-of-machine-intelligence.

Athey, S., C. Catalini, and C. Tucker. 2017. "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk." Technical Report, National Bureau of Economic Research.

Bertocchi, G., and A. Dimico. 2014. "Slavery, Education, and Inequality." *European Economic Review* 70:197–209.

Chiou, L., and C. E. Tucker. 2014. "Search Engines and Data Retention: Implications for Privacy and Antitrust." MIT Sloan Research Paper no. 5094-14, Massachusetts Institute of Technology.

Custers, B., T. Calders, B. Schermer, and T. Zarsky. 2012. "Discrimination and Privacy in the Information Society." In *Volume 3 of Studies in Applied Philosophy, Epistemology and Rational Ethics* Berlin: Springer.

Datta, A., M. C. Tschantz, and A. Datta. 2015. "Automated Experiments on Ad Privacy Settings." *Proceedings on Privacy Enhancing Technologies* 2015 (1): 92–112.

Dietvorst, B. J., J. P. Simmons, and C. Massey. 2016. "Overcoming Algorithm Aversion: People Will Use Imperfect Algorithms If They Can (Even Slightly) Modify Them." *Management Science* https://doi.org/10.1287/mnsc.2016.2643.

Farrell, J. 2012. "Can Privacy Be Just Another Good?" *Journal on Telecommunications and High Technology Law* 10:251.

Goldfarb, A., and C. Tucker. 2012. "Shifts in Privacy Concerns." *American Economic Review: Papers and Proceedings* 102 (3): 349–53.

Kosinski, M., D. Stillwell, and T. Graepel. 2013. "Private Traits and Attributes are Predictable from Digital Records of Human Behavior." *Proceedings of the National Academy of Sciences* 110 (15): 5802–05.

Lambrecht, A., and C. Tucker. Forthcoming. "Algorithmic Discrimination? Apparent Algorithmic Bias in the Serving of Stem Ads." *Management Science*.

———. 2013. "When Does Retargeting Work? Information Specificity in Online Advertising." *Journal of Marketing Research* 50 (5): 561–76.

———. 2017. "Can Big Data Protect a Firm from Competition?" *CPI Antitrust Chronicle*, Jan. 2017. https://www.competitionpolicyinternational.com/can-big-data-protect-a-firm-from-competition/.

Marthews, A., and C. Tucker. 2014. "Government Surveillance and Internet Search Behavior." Unpublished manuscript, Massachusetts Institute of Technology.

McDonald, A. M., and L. F. Cranor. 2008. "The Cost of Reading Privacy Policies." *Journal of Law and Policy for the Information Society* 4 (3): 543–68.

Miller, A., and C. Tucker. 2017. "Privacy Protection, Personalized Medicine and Genetic Testing." *Management Science*. https://doi.org/10.1287/mnsc.2017.2858.

———. 2018. "Historic Patterns of Racial Oppression and Algorithms." Unpublished manuscript, Massachsetts Institute of Technology.

O'Neil, C. 2017. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Portland, OR: Broadway Books.

Rubinstein, A. 2006. "Discussion of 'Behavioral Economics.'" Unpublished manuscript, School of Economics, Tel Aviv University, and Department of Economics, New York University.

Sokoloff, K. L., and S. L. Engerman. 2000. "Institutions, Factor Endowments, and Paths of Development in the New World." *Journal of Economic Perspectives* 14 (3): 217–32.

Strotz, R. H. 1955. "Myopia and Inconsistency in Dynamic Utility Maximization." *Review of Economic Studies* 23 (3): 165–80.

Sweeney, L. 2013. "Discrimination in Online Ad Delivery." *ACM Queue* 11 (3): 10.

Tucker, C. 2014. "Social Networks, Personalized Advertising, and Privacy Controls." *Journal of Marketing Research* 51 (5): 546–62.

Varian, H. R. 1996. "Economic Aspects of Personal Privacy." Working paper, University of California, Berkeley.

Warren, S. D., and L. D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193–220.