6 May 2015

Consumers as Data Brokers:
Should They Sell Their Own Personal Data?

W231-1: Legal, Policy, and Ethical Considerations for Data Scientists
Spring 2015
Final Project Paper
Tony Abraham | Marguerite Oneto

1. Introduction

In today's digitally-networked world, we are constantly leaking data. Every web search is catalogued. Every social media interaction is recorded. Every cell phone emits its GPS location. Companies are collecting this data at their leisure, using their terms of service and privacy policies to quietly acquire consumers' passive consent. Consumers are in the dark about what information is collected about them, how it is used, and what it is worth. How much money do these companies make by selling consumers' personal data? As Michael Fertik, CEO of Reputation.com, says,

> The basic business model of the Internet today is that we're going to take your data without your knowledge and permission and give it to people that you can't identify for purposes you'll never know.[1]

Can consumers revoke their consent and take back control of their own data by selling it directly to companies themselves?

There are many issues involved in undertaking such an approach. Can a direct personal data market (DPDM) actually be implemented? What are the implications of consumers selling personal data directly to data collectors? Do these implications warrant government protection or regulation?

We first look at the feasibility of creating a direct personal data market.

2. The Direct Personal Data Market

In our research, we found four companies that specialize in creating a direct marketplace for personal data. These companies are Beagli, Datacoup, Handshake, and Meeco. Each company offers unique services in order to differentiate themselves in the market, and each company has their own business model for leveraging user data.

2.1 Companies in the Industry

Beagli is an English company whose slogan is "Your data is your asset."[2] The company is currently in the beta stage of production, but their website details their eventual offering. Beagli collects data by having its users link up a proprietary mobile application to social media accounts and the phone's sensors, including the gps and accelerometer. The company also offers a desktop web browser plugin to monitor their users' browsing habits and patterns. The platform then combines all of the social media data, web history, activity data, and environmental data into the user's profile. Beagli creates revenue by brokering the transaction of these profiles (or portions thereof) between brands and its users in an auction format. The users have the option to accept or decline each offer, and they can automatically decline offers from brands they do not like. Beagli's encryption and security are based on Amazon Web Service's basic security protocols, which have their own independent terms of service.[3] Beagli

[1] Simonite, Tom. "If Facebook Can Profit From Your Data, Why Can't You?" MIT Technology Review. July 30, 2015.
[2] Beagli. https://beagli.com/ 2014
[3] Beagli Privacy Policy. https://beagli.com/legal 2014

requires all brands that purchase data to keep user information "secure at all times" through a legal data sharing agreement.[4] Finally, if a user wants to completely remove their data, Beagli offers an account deletion option, but they warn that complete deletion of personal data and backups requires an indefinite amount time.

Datacoup is based out of New York City, and it is the only American direct personal data market we encountered in our research. Datacoup's slogan is "Reclaim your personal data."[5] Datacoup's data marketplace is presently in operation, and the company itself was established in June 2012.[6] Datacoup offers a web portal where users can connect their social media accounts and financial information directly to the platform. Datacoup is the only DPDM we discovered where users can grant the platform read-only access to their credit card and banking accounts. After a user connects their accounts, Datacoup rates the user's profile and estimates the profile's total value and the value of each of its active data points. Brands can view all of the profiles and decide which users they want to analyze in depth. Datacoup rents this data to the brand on a weekly basis, and informs the user when their data is included in this transaction. Datacoup's security relies on firewalls and data encryption, and it uses read-only tokenized access to user financial accounts, which prevents any unauthorized transactions in the case of a data breach.[7] Datacoup allows its users to terminate their membership, but it is unclear whether or not their personal information will remain stored on Datacoup's servers.

Handshake is a British company that aims to help users negotiate a price for their personal data. Handshake's slogan is "Your data belongs to you. So when it is sold, you should be the one that benefits."[8] Handshake was established in 2013 and they are currently in beta, but the site itself has not been updated since that time. In article from National Public Radio, Handshake as launching its platform in the summer of 2014, but it is unclear if they successfully met that target.[9] Handshake offers a mobile application where users populate a data profile that serves as the basis for transactions. Brands will then contact users in whom they're interested and bid on the data they have available. These bids may also require the user to provide additional information via surveys or other app functionality like GPS. Users always have the option to deny the bid if it's too low or if they do not like brand involved in the transaction. Handshake offers "industry-standard" security practices, and it claims to achieve the SSAE 16 standard and ISO 27001 certification.[10] Finally, Handshake allows users to terminate their account and delete their profile through their online portal.

Meeco is an Australian company with the slogan "Collaborate with the people you trust."[11] The company was established in 2013, and their platform launched in the summer of 2014. Based on the information found on their website, Meeco could be classified as an emerging social

---

[4] *Id*.
[5] DataCoup - Reclaim your personal data. http://datacoup.com/ 2015
[6] Brewster, T. (2014, September 5). Meet Datacoup - the company that wants to help you sell your data. Retrieved April 19, 2015
[7] DataCoup Terms of Service. https://datacoup.com/docs#toc 2015
[8] Handshake - What's your worth? http://handshake.uk.com/ 2013
[9] Palet, L. (2014, September 9). Privacy Or Profit? These Firms Want To Help You Sell Your Data. Retrieved April 19, 2015
[10] Handshake - Frequently Asked Questions. http://www.handshake.uk.com/hs/faq.html 2013
[11] Meeco - Sovereignty for All. https://meeco.me/ 2013

network where users record their buying preferences, favorite brands, frequently visited websites, and communication habits. The outcome of these interactions is gathered into a dashboard that gives the user insight into their own routines and patterns. Unlike Beagli, Datacoup, and Handshake, Meeco does not attempt to directly monetize user data. Instead, Meeco creates an environment where users benefit from the knowledge of their personal data while receiving customized discounts and personalized deals from brands to which they have subscribed. Meeco focuses on allowing users to opt-in on brands they like, rather than opting-out of brands they do not like, which is the experience offered by Beagli and Handshake. As an Australian company, Meeco touts the advanced privacy laws of Australia, with which it complies, as well as describing using encryption and PIN numbers for added security.[12] If a user decides to remove their data, Meeco will purge the data from their site.

2.2 Practical Feasibility of the Industry

In order to establish a sustainable industry for direct personal data markets, Beagli, Datacoup, Handshake, and Meeco will need to overcome several practical challenges. The first is to adequately convince consumers that it is worthwhile to produce and sell their data on these platforms. Subsets of this challenge include convincing users of the security of their data and the full control that users will have over the data itself. The second challenge is persuading brands and customers that the data available is valuable enough to purchase. Brands are currently obtaining data on their customers via existing channels; companies with direct personal data markets will need to persuade the brands of the superiority and economic value of their data. Finally, it is a challenge for such a nascent industry to survive with the segmentation that it currently exhibits.

Beagli, Datacoup, Handshake, and Meeco must first convince potential users that direct personal data markets are worthwhile endeavors. The primary way is convincing users of the benefits, usually monetary rewards that users will receive on these marketplaces. The exact dollar amount that a user could receive varies by the platform and source of the information. Datacoup estimates that a user could make $8 a month for sharing their social profiles.[13] Handshake estimates that users could make over £400 a month for the most active users. Additionally, Handshake offered a 10% share in their company to the first 2,000 people who signed up to beta test their platform.[14] In order to entice actual users to their platforms, these companies must first clearly establish exactly how much a user should expect to receive for their involvement.

The direct personal data markets must also clearly define their security practices. In our research of these companies, we found minimal information about how the data was stored and encrypted. Beagli leaves the responsibility of security to its data provider, Amazon Web Services.[15] Handshake described their auditing standards rather than the technology they use to encrypt and secure their data.[16] Meeco describes stricter data restrictions found in its home

[12] Meeco - Privacy Policy. https://meeco.me/privacy.html 2014
[13] Palet, L. (2014, September 9).
[14] Lomas, N. (2013, September 2). Handshake Is A Personal Data Marketplace Where Users Get Paid To Sell Their Own Data. Retrieved April 20, 2015.
[15] Beagli Privacy Policy. https://beagli.com/legal 2014
[16] Handshake - Frequently Asked Questions. http://www.handshake.uk.com/hs/faq.html 2013

country of Australia, but it does not explain how those are implemented on its data.[17] Datacoup provides the best description of the security practices, but they may overestimate their effectiveness. For example, Datacoup touts the security of read-only access to financial accounts should there be a data breach, but they do not acknowledge the dangers of a stranger's knowledge of a user's spending habits.[18] Additionally, no company that we researched describes what would happen in the case of a data breach and how they would reimburse their users for a loss of their data.

Once the direct personal data markets obtain an adequate user base, they must convince brands that their available data is a commodity. There are many providers that currently sell personal data to brands. Established data brokers like Acxiom, Epsilon and Experian have been selling data to companies for decades.[19] Additionally, internet corporations like Facebook have similar services to help brands target current and potential customers.[20] These direct personal data markets will have to compete with these established companies in order to find success.

There are aspects of the data provided by these direct markets that brands could find enticing. Established data brokers provide data that has been aggregated from multiple sources. As a result, some of this data may be outdated or inaccurate. Data provided through personal data marketplaces was compiled by the primary source, namely the user him or herself. Additionally, the act of collecting data in such a manner would be a marketing coup for many brands. Much like companies that advertise products that were not tested on animals, companies that use data from personal data marketplaces could inform their users of that fact. This type of communication could engender trust and popularize the use of "ethically" harvested data.

After convincing brands of the value in this data, these direct personal data markets will need to compete against each other to establish standards and successful business models before the industry matures into sustainability. Presently, only Datacoup and Meeco are in production, and their early presence gives them an advantage in creating standards. Beagli and Handshake, while still in beta, share many aspects of their business models. If one were to launch successfully, it would be unlikely that they would both thrive. With that in mind, it could be that a failure of their business model has prevented them both from entering production.

3. What Are the Implications of Selling Personal Data?

It seems obvious that the number one threat of selling personal data is to privacy. Specifically, when consumers sell their data, do they sell away their privacy rights?

At first, it seems that once the sale is direct from consumers to data collectors, the consumer would be relinquishing control of how the data is used from that point forwards. Usually a data collector has a privacy policy that limits the downstream uses of that data. But with a direct sale, there would be no protection afforded from a data collector's privacy policies.

But advocates of personal data markets claim that they will give the individual more control

[17] Meeco - Privacy Policy. https://meeco.me/privacy.html 2014
[18] DataCoup Terms of Service. https://datacoup.com/docs#toc 2015
[19] Palet, L. (2014, September 9).
[20] Facebook Advertising - How it works. https://www.facebook.com/advertising/how-it-works 2015

over their privacy. This is because the current privacy policies of data collectors are blanket policies. They are the same for everyone, no matter what an individual's privacy preferences might be. When the sale is direct, consumers will have the right to structure these contracts as they see fit, using something akin to limited use licenses, as seen within intellectual property law.

Privacy as a subject is difficult because each individual has a different definition of what privacy means to them. In other words, people have privacy preferences. Ideally, each individual would relinquish his data to data collectors on his own terms according to his preferences. But the personal data markets are currently incomplete. The start-ups mentioned above are attempting to correct this imbalance of power, but they are just in the nascent stages.

Once these personal data markets mature and individuals can structure their sales contracts in any way they desire, will the markets cure the privacy problem, allowing individuals to reveal as much or as little about themselves as they desire? First, we must consider the current state of the privacy market.

4. The Privacy Market

In his paper "Property, Privacy, and Personal Data"[21], Paul Schwartz discusses the "privacy market." The market is driven on the supply side by individuals' preferences for more or less privacy. The demand side is driven by data collectors' ability to use personal data to generate profits. What is the product sold? In this framework, the sale of one's personal data is equivalent to the sale of one's privacy. Therefore, individuals are selling their privacy, while data collectors are buying personal data.

Schwartz goes on to characterize a well-functioning privacy market as one where individuals have the ability to "price discriminate" based on their privacy preferences. Price discrimination in this context is different from that in economics. Economists define price discrimination as the ability of sellers to charge different prices to different buyers according to the buyers' willingness to pay, or more specifically, according to the buyers' preferences. In the privacy market, price discrimination is the ability of different individuals to charge the same data collector different prices for their personal data depending on how much the individuals value the privacy of that data. In other words, an efficient privacy market allows individuals to sell their data for how much their privacy is worth to them.

Today's privacy market is patently inefficient. In most cases, individuals are only given a binary choice when it comes to selling their personal data. No matter how much individuals value their privacy, they either sell it for the stated price (for example, for specified access to a free online service like social media) or they don't sell it at all. Because individuals have different privacy preferences, they have different reservation prices for selling their data. The reservation price is the price that an individual places on not selling his personal information. Thus, an individual will ideally not sell his personal information unless he is offered more than his reservation price, whether that is paid in cash, goods, or services.

[21] Paul M. Schwartz (2004), "Property, Privacy, and Personal Data", Harvard L. Rev., Vol. 117, No. 7, 2056, p. 2076.

Why is the privacy market currently stuck in this inefficient equilibrium?

5. Causes of Privacy Market Inefficiency

The causes of inefficiency in the privacy market fall into two main categories. First, there are the inherent qualities of personal information: alienability, nonrivalrous consumption, and nonexcludability. Second, there are environmental factors that affect the functioning of the market: an incomplete legal framework, no superior claim to data control, technological advancements, and asymmetric information.

5.1 Alienability

Free alienability is the ability of property to transfer ownership without restriction. This is a fundamental requirement when selling goods, and it allows buyers to sell property that they previously purchased. In the realm of privacy markets and personal data, the validity of alienability immediately comes into question.

According to Schwartz (2004), there are three main problems with free alienability and information privacy[22]. With free alienability, a seller is prohibited from limiting the buyer in the use or transfer of the goods. This principle would be difficult to achieve in privacy markets. Users who sell their data once would find no future benefit, as the data could be disseminated by the first buyer to all other buyers. The second issue is "the difficulty in setting an appropriate price for secondary uses of one's personal data."[23] With this issue, a seller will be unable to determine a definitive price point for their data because buyers can use their data in a variety of ways. The third main problem is that if free alienability were applied to information privacy, the resulting policies that emerged to deal with the first two problems would likely over-regulate the market and block data trade as a result.

5.2 Public Good Qualities

Public goods are those that provide a benefit to society as a whole and have two particular qualities: no one can effectively be banned from using the good (nonexcludability) and the use of the good by one person does not diminish the availability of the good to others (nonrivalrous consumption). Classic examples are national defense and clean air.

Many scholars argue that the existence of privacy provides a benefit to society as a whole. In particular, privacy ensures that individuals can act as autonomous beings, which is a prerequisite for a democratic polity.[24] But privacy also suffers from nonexcludability and nonrivalrous consumption. If a society holds privacy as a fundamental right, backed up by the force of law, then no one can be excluded from its legal protection. In this sense, the government must allow everyone equal access to privacy, just as it allows everyone equal access to national defense. Furthermore, if one person sells his personal data (i.e. uses his privacy), this does not decrease the ability of another person to sell her personal data (i.e. does

[22] *Id*, p. 2055.
[23] *Id.*
[24] See, for example, Schwartz *supra* note 21, p. 2084, and Julie E. Cohen (2000), Examined Lives: Informational Privacy and the Subject as Object, 52 Stanford L. Rev. 1373, p. 1426.

not decrease the availability of privacy to her).

Public goods are usually provided by the government or are highly regulated by it. This is because they are notoriously mispriced by the market. Since no one can be excluded from their use, there is a free-rider problem. If there is no way to prevent someone from using it, why would that person pay for it? And if no one will pay for it, why would anyone produce it? Thus, if left to the markets, public goods would be overused and underproduced.

Today, many consider privacy underproduced and overused. It is underproduced in the sense that more and more individuals are trading their personal data for goods and services. They do not keep their privacy under wraps for the larger sake of a democratic society because there is no individual cost to doing so. That is, even if individuals trade their data, they are still eligible for legal recourse if they ever feel that their privacy has been violated.

Privacy is overused in the sense that the more people give up their data, the more surveillable society becomes. This is especially true with the current advances in data science. Data scientists, if given large enough amounts of data, can now take de-identified data and re-identify it. It is becoming increasingly difficult for individuals to find anonymity within a crowd.

These overall costs of diminished privacy are not taken into account in the privacy market. Thus, the market is unable to allocate the proper amount of privacy to a society. There is an inefficient allocation of this public good.

5.3 Incomplete Legal Framework

Despite over 100 years of developing legal doctrine for privacy protection, there is still an incomplete legal framework for privacy rights. In *Markets and Privacy*, Laudon states that privacy rights in the United States rest on common law, the constitution and its amendments, and statutory law[25]. There are dramatic legal shortcomings in each approach to privacy. Common law claims for privacy protection "interfere with constitutional protection of free speech and expression,"[26] and the claims are more successful for celebrities than they are for ordinary citizens. Constitutional amendments allow for freedom of expression, beliefs, and home property, but they do not cover any private information or data revealed in "professional or business transactions."[27] Finally, the statutory law enacted by states is "confusing, piecemeal, and riddled with loopholes."[28]

5.4 No Superior Claim

As we can see in Section 5.3, our legal system dares not define which has the superior claim, disclosure of information or privacy.

Our society values both disclosure of information and privacy. On the one hand, we believe the

[25] Laudon, Kenneth C. (1996), "Markets and Privacy," Association for Computing Machinery. Communications of the ACM 39, p. 94.
[26] *Id*.
[27] *Id*, p. 95.
[28] *Id*.

more information that is available, the better off we are. More information leads to the more efficient provision of government benefits, to more individualized delivery of goods and services, to faster development of new drugs and medical therapies, and to the delivery of more free personalized services such as internet search and social networking.[29]

On the other hand, we value privacy for its ability to support individual autonomy and democratic principles, as mentioned above. Privacy also allows us to avoid some additional, often overlooked costs.[30] When privacy is diminished, individuals must expend additional resources to safeguard their personal information, such as encrypting correspondence or erecting physical barriers. Additional resources are also expended when individuals must defend their reputations if correct but incomplete information is disclosed about them. The fact that we don't take these often overlooked costs into account, which could be remedied with the existence of a superior claim rule, leads to inefficient privacy market outcomes.

5.5 Technological Advancements

The extreme rate of technological advancement has made it difficult to enact sustainable legislation and standards in the technical realm. Regarding privacy markets, some applicable standards are upwards of 50 years old. Laudon describes the FIPPs doctrine and its "no secret systems" principle as outdated and damaging to modern ideas of privacy. He states that the number of modern databases has made it impossible for an individual to "gain access, review, or correct information." He also states that it's impossible to give "informed consent" for one's data, and its impossible to know if that data is properly secured on a third party's server.[31] Clearly, these basic needs are the foundation of an effective privacy market.

5.6 Asymmetric Information

It is obvious that data collectors have better information than individuals do about what personal data is being collected, how it is being used, and how much it can sell for. This asymmetry in information leads to classic adverse selection and moral hazard problems.

In the privacy market, adverse selection means that there is a race to the bottom. Companies that are responsible stewards of the personal information they collect have no way to signal to individuals how responsible they are. Their privacy policies might reflect it, but in today's privacy market individuals are not in the habit of reading these paragons of legalese. Because these companies can receive no reward for their responsible stewardship, they have no incentive to continue to protect personal data. The privacy market ends up in a lemons equilibrium, where all companies are assumed to be bad stewards of private information.

Moral hazard arises because individuals cannot detect whether companies are violating their privacy agreements. First, individuals do not even know or understand what is included in most companies' privacy policies. Second, even with today's technology, it is prohibitively expensive in terms of time and money for individuals to monitor those who collect their private

[29] "Personal Data: The Emergence of a New Asset Class" (2011), The World Economic Forum, p. 5.
[30] Richard S. Murphy (1996), "Property Rights in Personal Information: An Economic Defense of Privacy," 84 GEO. L.J. 2381, p. 2396-2402
[31] Laudon, *supra* note 25, p. 96

information. There is a standard principal-agent problem.

If an individual agrees to a company's privacy policy, that company becomes the principal of the individual. And as a principal, the company is responsible for protecting the individual's privacy. The problem is that the principal's interests are not aligned with the agent's interests. The principal has strong financial incentives to sell the agent's personal data, but it is the agent who bears the brunt of the costs to his privacy. Therefore, the privacy market ends up in an equilibrium where the principal sells more personal information than the individual would prefer.

6. Solutions to Privacy Market Inefficiency

There are many privacy scholars who study this phenomenon of inefficiency, and each has his or her own theories about the solutions to the problem. One cohort argues that granting personal information a property right is the answer to privacy market inefficiencies. Another argues that claiming personal data is property will diminish the ability of individuals to protect their privacy and that there exist better legal remedies.

In the following section, we compare and contrast these two approaches to privacy market problems.

6.1 The Property Approach

There is a school of thought that says that individuals should own their personal data, or in other words, have a property interest in their data. But how to characterize this interest and protect it in the privacy markets, as well as in the courts, is up to much debate. In this section, we review several of the ways that property is defined for personal data and what additional constraints need to be put in place to make these property definitions effective.

6.1.1 A Bundle of Interests

Schwartz (2004) subscribes to Hohfeld's definition of property as a bundle of interests. He claims that "the understanding of property as a bundle of interests rather than despotic dominion over a thing helps frame a viable system of rights with respect to personal data."[32] In the case of personal data, what should be included in this bundle and to whom should each interest be granted?

The first interest is a hybrid inalienability that is awarded to the individual. This hybrid consists of three parts: a use limitation, a transfer limitation, and an opt-in default. As Schwartz describes it,

> In practice, it would permit the *transfer* for an initial category of *use* of personal data, but only if the customer is granted an opportunity to block further transfer or use by unaffiliated entities. Any further use or transfer would require the customer to opt in -- that is, it would be prohibited unless the customer

[32] Schwartz, *supra* note 21, p. 2094.

affirmatively agrees to it.[33]

This model creates multiple rounds of negotiations between individuals and data collectors, in stark contrast to today's one-and-done deals. And at each round of negotiations, data collectors would be forced to reveal more information to sellers. This would enable individuals to set more optimal prices for their privacy, i.e. make it easier for them to reach their reservation price.

This more efficient pricing would solve some other market failures. It would allow individuals to see the true cost of selling away their privacy and induce them to sell less. This is because today's opaque privacy market allows secondary users to pay less than what the information is truly worth to the individual. This would help cure part of the public goods problem of underproduction of privacy in society. Better pricing would also decrease the potency of the moral hazard issue associated with asymmetric information. It would prevent primary data collectors from selling more information to secondary users than the individual would prefer.

Schwartz acknowledges that his hybrid inalienability would require some additional safeguards. First, the government would need to be involved in regulating how privacy terms are disclosed to individuals, making sure that the terms are clear and concise. Second, some kind of nonpersonal metadata that outlines the agreed upon terms of that data's use and transferability must be attached to personal data, perhaps through a bar code. This would allow third-party users of the data to verify and adhere to its limitations.

The second property interest in personal data is the right to exit previous sales agreements. This right is granted to the individual and would prevent the long-term consequences of a bad privacy trade. It would allow individuals to punish data collectors who are deceptive in their privacy practices or who do not adhere to their promises. Further, individuals could exit trades in order to take advantage of new, more privacy-friendly opportunities. This would help individuals come closer to reaching their reservation price, as well as encourage innovation in privacy practices and technologies that increase personal data protection.

The final property interest in personal data is the right for individuals to sue for liquidated damages inflicted by breaches in privacy contracts. What is unique here is that the liquidated damages would be determined by the government, not by the buyer and seller at the time they contract. The government would set these damages according to the difficulty in detecting such breaches -- the lower the probability of detection, the higher the fines will be. The role of the government is to set fines high enough so that it is worth the individual's effort to bring a lawsuit and so that it is worth the data collector's effort to keep its privacy commitments. This new right to government-determined damages would help to reduce moral hazard as the data collector's interests in protecting privacy become more aligned with those of the individual, as well as offset the detection and monitoring costs incurred by individuals.

To support these new property interests, Schwartz outlines the need for decentralized institutions to develop to serve three primary functions within the privacy market: 1) to provide trading platforms (a market-making function); 2) to authenticate the terms of a data

[33] *Id*, p. 2098.

trade (a verification function); and 3) to police compliance with both private contracts and government mandates (an oversight function). As outlined in Section 2, we see recent, innovative additions to the market-making function that should, according to Schwartz, help the privacy market achieve more efficient outcomes.

6.1.2 A National Information Market

Laudon[34] also calls for a mix of market forces and regulation. But in contrast to Schwartz, he believes the market-making function should be centralized into a National Information Market. How does he come to this conclusion?

Laudon starts by noting that enforcement of legal privacy protections is solely on the shoulders of the individual, who must seek redress in the courts. This convention was systematized in the HEW Report of 1973, where the Advisory Committee recommended that privacy laws be enforced by individual court actions. The report also acknowledged that individuals have an interest in the data collected about them, but it did not delineate what that interest is. In particular, the Advisory Committee did not call it a property interest.

Furthermore, as outlined above in Section 5.5, technological advancements have rendered the HEW Report's Fair Information Practice Principles (FIPPs) impotent. But it is truly our lack of a proper institutional structure that allows privacy invasion, not technology. Laudon points out, "We tend to blame technology for what is an institutional situation we have created."[35] Laudon proposes several new institutions that should be formed to remedy this. The primary one is to declare an individual property interest in personal data. This would make the use of personal data without consent a crime and would close the loopholes in the incomplete legal framework surrounding privacy.

The second institution needed to create better guarantees of privacy is a National Information Market (NIM). The goal of the NIM would be to allow transactional data (primary use data) to be sold by individuals at a market-clearing price for secondary use by commercial interests. Practically, individuals would "deposit" their personal information at a local information bank. The information would then be forwarded to a centralized database, the National Information Exchange. Institutions could then purchase the data from the exchange, granting them rights to use it for a limited amount of time.

The NIM would be the only place where institutions can purchase personal information for secondary uses. This centralization would ensure that individuals receive some monetary compensation for each use of their data. It would also create a digital audit trail where individuals could look up how a particular entity received their information.

Centralization would ensure that external costs that make the privacy market inefficient, such as overuse of privacy, employing encryption, and defending reputations that have been compromised, are completely internalized. Such a statement implies that today's decentralized direct personal data market ultimately cannot achieve efficient market outcomes.

---

[34] Laudon, *supra* note 25.
[35] *Id*, p. 99.

6.1.3 Privacy as Property

Although Laudon outlines the shortcomings of FIPPs in today's digitally-connected world, Mell (1996)[36] makes a case for building property rights on top of a FIPPs foundation.

Today's digital world has created what Mell calls the "electronic persona." This is a disembodied you, living inside databases that you do not control. It is an autonomous extension of yourself. It is "[a] personal information file electronically stored, which, by virtue of at least one 'identifier,' relates the personal information to a specific person."[37]

Mell defines privacy in terms of this persona, using the five principles outlined in FIPPs:

> [P]rivacy is the legally recognized power of an individual (group, association or class) to both 1) regulate the extent to which another individual (group, class, association or government) may access, obtain, make use of or disclose a persona concerning him ... and 2) monitor and correct the accuracy of the persona compiled concerning him.[38]

Within common law, privacy is considered an inalienable right, and although it can be waived, it cannot be sold, transferred, or appropriated. But because the electronic persona exists separately from the individual, in multiple government and private databases, it becomes alienable. And as the persona is alienated, so is the individual's privacy. Mell states, "In this manner, privacy and property meld in the electronic milieu."[39]

Mell thus advocates for a reconsideration of the nature of privacy and property in the digital age in order to specify exactly how alienability should be defined for personal data, as embodied in the persona, so that individuals can maintain control of their identities and privacy. In particular, she calls for the electronic persona to be declared as property, with the "ownership" or "fee simple" rights conferred solely on the individual. This does not deny that others have an interest in the persona (government, the public, commercial entities), but it subordinates these interests to the individual's property rights. Ultimately, this means that any data collector must bargain with the individual to gain consent for use of his personal data.

In order to instill this property right in the individual, Mell requires that a law be passed, the "Uniform Electronic Persona Protection Act."[40] It would establish a principle-agent relationship between the individual and the data holder. The data holder, as agent, would have the duties embodied in a double warranty that is in line with FIPPs: a warranty of authority to disclose the data and a warranty of accuracy of the data.[41] The individual, as principle, would be given the opportunity to see the personal data that would be disclosed about him before any such

---

[36] Patricia Mell (1996), "Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness," II BERKELEY TECH. L.J. I, 26-41.

[37] *Id*, p. 4.
[38] *Id*, p. 10.
[39] *Id*, p. 71.
[40] *Id*, p. 85.
[41] *Id*, p. 79.

disclosure, allowing him to correct the information if necessary.

The statute would have some additional provisions, such as granting a limited use license to government for its matching programs, requiring those testifying in confidential investigations to swear to the truth of their testimony involving personal information, and obligating data holders to specify each employees access rights to any personal data.

All of these provisions of the Uniform Electronic Persona Protection Act would establish the parameters of alienability surrounding personal data. This would help to increase the efficiency of the privacy market by closing the loopholes inherent in our current legal framework.

6.1.4 A Technology Solution: P3P

Lessig (1999)[42] also contends that more consequential collective, political action is needed to give individuals a meaningful choice when it comes to divulging their personal information within the digital world because the current personal data market has proven itself unable to do so. In particular, he looks to copyright as a model for how to allocate rights to individuals regarding their personal data.

Copyright admits what is called a derivative right. This gives the holder of the derivative right the legal ability to build upon a copyrighted work. In some instances, the copyright owner has a property right over the derivative right: anyone who wishes to obtain a derivative right must pay the copyright owner whatever price he may ask. Furthermore, the copyright owner may limit the number of people who can have derivative rights.

In other instances, the copyright owner is only given a liability right over the derivative right: anyone can obtain a derivative right without the copyright owner's consent simply by paying a set statutory price. The copyright owner cannot price discriminate, i.e. charge different entities different prices for the same derivative right. He also cannot limit the number of people who can have derivative rights.

Lessig calls for the enactment of a property right in personal information instead of a liability right precisely to give individuals the power to price discriminate according to their personal privacy preferences. Historically, this is what the property vehicle was designed to do.

Lessig contends that this new property right cannot be effective on its own. It must be combined with new architectural elements built into the internet. One particular technology solution is P3P (Platform for Privacy Preferences Project). This platform essentially allows individuals to embody their privacy preferences in an electronic file which could be read by any website with which individuals interact. When accessing the website, a comparison would be run between the privacy preferences of the individual and the privacy policies of the company. If the two do not match, then the individual would have the option to change his preferences to match the company's or else leave the website.

P3P would solve the market's inability to allow price discrimination according to personal

[42] Lawrence Lessig (2006), "Code, Version 2.0." Downloaded under the Creative Commons Attribution-ShareAlike 2.5 License on April 28, 2015 at http://www.codev2.cc/download+remix/Lessig-Codev2.pdf.

privacy preferences by making it clear to individuals the price that each website is willing to pay to buy their personal information. They can then decide whether or not to sell it for that price. It would also solve some of the asymmetry in information by making privacy policies explicit and detailed without the legalese.

But P3P has already been tried and abandoned (its only large adopter being Microsoft). Perhaps this is because the property law Lessig calls for has not been implemented, leaving it to the personal data market to decide voluntarily if they will implement P3P. Given that the overall market has been left unfettered, perhaps a better, viable solution is the direct personal data market.

6.1.5 The Superior Claim

Murphy (1996)[43] uses economic arguments to prove the point that privacy should always have the superior claim over data disclosure. This is true whether the original information is given to the data collector voluntarily, as is the case in the direct personal data markets, or involuntarily, without consent, as is the case with surveillance.

Murphy starts by stating simply that personal data is property. The sole concern of the law should be to decide how to allocate the property rights between the subject of the personal data and the collector of the personal data. This entails defining who has the superior claim over disclosure of the data, i.e. setting a default rule as to who is allocated the property right at the time the action that generates the personal data occurs.[44]

For involuntarily-given information, the common law tort of invasion of privacy developed by Brandeis and Warren proved ineffective and was eventually replaced by Prosser's four causes of action: false light, appropriation, intrusion, and disclosure.[45] But even Prosser's distinctions do not always obtain the most efficient privacy outcomes. This is because tort law establishes objective norms of civility that pertain across all individuals, which inherently does not take into account the range of privacy preferences in society. Murphy says, "If, however, … the depth and diversity of privacy preferences are highly variable across individuals, the objective approach will often get it wrong."[46]

Because this information is involuntarily given, there is no contract we can turn to in order to determine the individual's privacy preference. What we can do is give the individual the superior claim over disclosure of his data, and if transaction costs are low enough, he can contract to sell his data for a price above his reservation value, if he sees fit to do so. This default rule will thus yield the optimal privacy outcome.

In scrutinizing the negotiations over voluntarily-given personal information, Murphy points out the general economic question that should be asked when deciding the most efficient default rule: On average, will the individual value his privacy more than the data collector values selling the individual's personal data? To get at an answer, Murphy suggests two more specific

[43] Richard S. Murphy (1996), *supra* note 30.
[44] Note that even though we are defining who should have a superior claim, i.e. a default rule, this does not preclude the parties from contracting around the claim.
[45] *Id*, p. 2389-2390.
[46] *Id*, p. 2393.

questions:

1. What are the relative transaction costs of contracting around the default rule?
2. Will the default rule correct an imbalance of information between the individual and the data collector?[47]

The answer to the first question is that the transaction cost an individual would incur to write a contract to prevent the data collector from selling his personal data is higher than the cost a data collector would incur to get an individual's consent to disclose his information. The data collector is writing the original contract and can just add a check-off box to it.

The answer to the second question is that there is an imbalance of information and the privacy default rule would correct it. The data collector always knows the value of the personal data because he is going to sell it, whereas the individual usually does not. The privacy default rule would force the collector to disclose at least some of this pricing information.

Given these two answers, Murphy decides that the default rule should always be to grant the superior claim to the individual and his privacy, just as is true with involuntarily-given information. In the end, defaulting to the individual property right in all cases leads to the most efficient, least costly, privacy outcome.

6.2 Alternatives to The Property Approach

Some scholars have subscribed to the idea that information is not private property. In her paper, *Privacy As Intellectual Property?*, Samuelson argues that the creation of a property rights market would immediately create "significant friction" with data markets that presently operate without such limitations[48]. In *The New Intrusion*, Bambauer states that if the government incorporated a property model into law, it would immediately face constitutional challenges to its legality[49]. Litman, in *Information Privacy/Information Property*, concurs with Bambauer and Samuelson, claiming that the creation of any property-based market would fail because of the inalienable nature of information and data.[50]

In the scope of the privacy markets, these scholars have proposed legal solutions as alternatives to the property-based model. These solutions range from practical to theoretical, but all offer a valuable perspective in devising a framework for an efficient and sustainable personal data market.

6.2.1 Licensing Framework

Samuelson proposes a licensing framework as a legal alternative to a privacy market grounded in property law. In her recommendation, Samuelson borrows from trade secrecy law for its shared interests in information privacy and ownership. Trade secrecy law has many benefits as a model, including default licensing rules, the ability to restrict access and usage of private

[47] *Id*, p. 2412.
[48] Pamela Samuelson (2000), Privacy as Intellectual Property?, 52 STAN. L. REV. 1125, p. 1137.
[49] Bambauer, Jane R., The New Intrusion (March 9, 2012). Notre Dame Law Review, Vol. 88, 2012; Brooklyn Law School, Legal Studies Paper No. 265.
[50] Jessica Litman (2000), Information Privacy/Information Property, 52 STAN. L. REV. 1283, 1283-1313.

information, the encouragement of commercializing information, and standards for commercial morality. Samuelson explores these benefits through three separate transactions: contractual agreements, disclosure of information in confidence, and unauthorized disclosure of information.

Contractual agreements occur when an individual or company agrees to give a recipient party access to confidential, nonpublic information. In this transaction, the recipient party must respect restrictions on the information, as well as abide by terms and conditions put in place by the individual. The "information... does not become 'public'," despite the number of parties with access because these recipient must first agree to maintain the private nature of the information.[51] A contractual transaction of personal data would allow a seller to restrict the buyer's use of the data, circumventing the challenge of free alienability that we outlined earlier in this document. Data transactions based on contractual agreements would also allow sellers to adequately price their data. It's easy to imagine a tiered approach to a data sale, where certain restrictions on the data are reduced at a higher price point. The feasibility and practicality of contractual agreements are visible in the business models of the direct personal data markets Handshake and Datacoup.

Disclosure of information in confidence takes place when an individual or company grants data access to a recipient party while maintaining restrictions on the use of the data. In Samuelson's example, a company grants a consultant access to nonpublic information on the condition that he use the data only to help improve the company's operations. The nonpublic information in this scenario "may have a commercial value beyond its utility to aid the consultant in doing his job," however, the consultant's use of the data must not extend beyond its original scope, and the consultant must not circulate the data to competitors or shareholders. "If licensor has provided data to another for a particular purpose, the data cannot be used for other purposes without obtaining permission."[52] Even without an agreement, the contractor understands that control over uses of the information always resides with the originator. This is immediately applicable to private data. Licensing personal data allows users to maintain control over how their data is used, with or without a contract in place. This again prevents the challenge of data and free alienability, and it allows users to restrict the number of customers who have access to their data.

Unauthorized disclosure occurs when a recipient party obtains access to nonpublic information and suspects that the information was obtained by "improper means, or in breach of confidence."[53] The firm or entity that owns the information may halt unauthorized use of the information by sending notice to the recipient party. In the realm of personal data markets, users can request data brokers stop using their data if they're not authorized, giving the users more control over their flow of data and recourse when their data is used inappropriately.

Samuelson acknowledges that a law for licensing personal data would not solve all of the information privacy problems, but such a model does provide the best path forward. Regardless of the final legal solution, Samuelson calls for a framework that does not copy some

[51] Pamela Samuelson (2000), Privacy as Intellectual Property?, 52 STAN. L. REV. 1125, p. 1152.
[52] *Id*, p. 1155.
[53] *Id*, p. 1157.

"pre-existing zone of privacy" from the physical world, as personal data markets have only recently come into existence.[54]

6.2.2 Tort Law Frameworks

Bambauer and Litman each propose legal alternatives that are guided by tort law. Bambauer focuses on the intrusion tort and the opportunity for an individual to seek redress for privacy harms. Litman explores the breach of confidence tort as a model for data ownership, primarily because it is "less likely to legitimize wholesale commercial exploitation of personal information."[55] Each author provides a unique perspective on tort law's role in data ownership, with varying degrees of impact in their proposed solutions.
In her paper, The New Intrusion, Bambauer segments information flow into four stages: "observation, capture..., dissemination, and use."[56] Dissemination and use of information are protected by First Amendment rights, so Bambauer avoids restricting those aspects of information flow. Instead, she focuses her proposed solution on the observation stage, which has protection under the intrusion tort. By reducing the classic intrusion tort to two elements: "(1) an observation, (2) that is offensive," Bambauer creates a focused model with unique protections.[57]

In the realm of data ownership, defining "observation" can be challenging. Bambauer sides with the Fair Information Practices to define observation as "personal data [that] is used or disclosed for some purpose inconsistent with its original collection without advance notice or consent."[58] Bambauer further defines observation as any time anonymized data is related back to the original device-user.[59] In the realm of privacy markets, observation would refer the use of an individual's data in consumer-based research or modeling.

Bambauer defines "offensive" as intentionally observing an individual who has a "reasonable expectation of seclusion."[60] In the realm of data markets, the idea of seclusion is evolving, but it could be simply defined as "a data-user who has not voluntarily disclosed her data."[61]

Combining the the definitions of "offensive" and "observation," it is very straightforward to formulate the act of unauthorized data use within the data market. If buyers use data that was obtained without the permission of its originator, the originator could seek redress via intrusion tort law. Although intrusion tort law may not apply immediately to data markets, Bambauer is confident, however, that the "courts have not had too much trouble knowing seclusion when they see it."[62]

Litman pursues breach of privacy tort as an alternative framework, but she proposes a much more extreme interpretation. Under this tort, the "reuse, correlation, and sale" of consumer

---

[54] *Id*, p. 1129.
[55] Litman, *supra*, p. 1312.
[56] Bambauer, *supra*, p. 205.
[57] *Id.*
[58] *Id,* p. 252.
[59] *Id*, p. 250.
[60] *Id*, p. 231.
[61] *Id*, p.249.
[62] *Id*, p. 233.

data without advance knowledge would constitute an actionable offense.[63] Litman argues that customer outrage regarding the sales of their personal information fulfills the requirements of breach of trust. As a result, applying breach of privacy to personal data transactions could altogether forgo the existence of "the privacy-rights-management market."[64] Litman concludes that breach of privacy tort law does not provide protection for individual data privacy currently, but she states that it is intuitive enough to be applied in the future should consumer outrage warrant it.

Both Bambauer and Litman conclude that tort law is a path to efficient data privacy ownership, but it will take a larger social change to become properly enacted. As a result, consumers may become more and more accustomed to observations on their data, and less likely to pursue protection in the realm of tort law.

6.2.3 Moral Foundation Alternative

Allen, in her article "Coercing Privacy," outlines an approach to data ownership that stands in the face of legislation and regulation of the market.[65] Allen argues that the privacy market constructs a desire or need for consuming other people's privacy. As a result, the market is self-feeding and eventually results in lower expectations for individual privacy rights. Allen posits that the best approach to data ownership would be education and a strengthening of the moral foundation of the population. If leaders could convince and empower consumers to "hold onto their own privacy and consume less of others'," they'd be more inclined to halt the steady decline of individual privacy rights.[66] This could potentially create a class of users who are reluctant to support businesses with less ethical data collection, ushering in a dawn of companies that tout their "ethically-harvested" data practices. By proposing a more organic approach to market change, Allen relies less on legislation and law and more on a ground-up approach to data ownership that was missing from the earlier legal alternatives. Still, Allen concludes that the moral approach may be the hardest to actively achieve.

7. Are Direct Personal Data Markets the Solution?

Direct Personal Data Markets are not immune to the privacy market inefficiencies outlined earlier in this paper. Implementations of DPDMs are relatively new, however, which allows them to build their business models off of years of literature and perspective in the space. As a result, there are inefficiencies that the direct privacy markets handle directly, and those they ignore.

Alienability: DPDMs handle the alienability inefficiency by instituting a licensing model for data transactions. Each of the DPDMs we researched have their own terms and conditions on data use, but a common requirement is a restriction on the redistribution of data. This requirement may be advertised as a means of securing user privacy, but the reality is that uncontrolled

[63] Litman, *supra*, p. 1308.
[64] *Id*, p. 1312.
[65] Anita L. Allen (1999), *Coercing Privacy*, 40 Wm. & Mary L. Rev. 723-757.
[66] *Id*, p. 735.

redistribution of user data would collapse the markets. By securing the free alienability of the data, the DPDMs can broker transactions between a single user and multiple brands, rather than the single initial sale of a user's data to the market as a whole.

Public Good Qualities: DPDMs will not help us get around the fact that privacy is nonexcludable and nonrivalrous. In the short run, it will likely exacerbate the problems of underproduction and overuse of privacy as early adopters rush in to try the novel services provided by Beagli, Datacoup, Handshake, and Meeco. But in the long run, individuals will get used to selling their data on their own terms and will revoke the consent that was previously given under companies' blanket privacy policies. This will make the privacy commons more protected, but not completely so.

Incomplete Legal Framework: Rather than waiting potentially decades or longer for the government to enact a proper legal framework for privacy rights, the DPDMs proceed in a legal environment beset with ambiguities and insufficient guidance.

No Superior Claim: Similar to ignoring the lack a legal framework in which to operate, the DPDMs offer no advancement to the superior claim inefficiency.

Technological Advancements: The rapid pace of technological advancements has prevented the legal system from maintaining equilibrium, but new technology also allows the DPDMs to create inventive solutions for other market inefficiencies. For example, the use of digital rights management (DRM) software on user data could prevent unauthorized distribution, or it could enact an expiration date on the data to coincide with the license expiration. Additionally, platforms like P3P allow users to restrict the amount of data that is collected outside of the DPDM, which could force brands to recognize the DPDMs as the most updated and legitimate source of user data.

Asymmetric Information: As DPDMs are perfected, they will completely dissolve the asymmetric information advantage that companies currently have with respect to the true value of an individual's personal data. Individuals will come to know exactly the price the market will bear for their information, as well as exactly how their information will be used. They will be able to ascertain which companies are good stewards of private information and which companies fall short of their expectations. This will give companies incentive to build reputations as privacy protectors, eliminating the current lemons equilibrium.

They will not, however, dissolve the policing problem that gives rise to the principal-agent problem. It will still be prohibitively costly for individuals to ensure that data collectors adhere to their privacy agreements. The solution for this will be technological advancement, as methods are devised to track the path of data as it passes from hand to hand through the personal data market.

8. Conclusion

It is an exciting time for personal data markets. In the past three years, multiple companies have emerged to directly offer individuals a platform for leveraging their personal data trail. Beagli, Datacoup, Handshake, and Meeco help their users create profiles that connect up key data points like their social media accounts, mobile devices, web browsing history, and even

financial statements. Once users have gathered an adequate amount of data, the platforms broker deals with brands to license their data for market research and user studies. As these Direct Personal Data Markets emerge and build their user bases, there are legal ambiguities regarding privacy ownership and market inefficiencies that must first be addressed.

There are many proposed solutions to the privacy market inefficiencies discussed above. The property approach entails defining a property right in personal information that accrues solely to the individual. This property right can be supported by a variety of different mechanisms, from a centralized National Information Market to a Uniform Electronic Persona Protection Act. From the technology of P3P to defining a superior claim or a bundle of interests. All of these proposals address some aspect of today's privacy market inefficiency.

Alternatives to the property approach include creating a licensing framework, refining tort law, and appealing to a moral foundation. The most promising licensing framework is grounded in trade secrecy law and its ability to restrict access and usage of private information. The benefits to individual privacy can clearly be seen in the trade secrecy definitions of contractual agreements, disclosure of information in confidence, and unauthorized disclosure. They all reduce the alienability of personal data.

Two of the most promising ways to refine tort law to protect privacy are to redefine the classic intrusion tort and to employ a more extreme interpretation of the breach of privacy tort. Both of these provide a path to efficient data privacy ownership. But appealing to a moral foundation may be the strongest way to protect individual privacy, although it might be the most difficult to implement.

The development of DPDMs is a bright light in the advancement of privacy rights, but it will not solve all privacy market inefficiencies. Our hope is that DPDMs find popularity and increase the public's knowledge about data ownership, while offering users immediate returns for their participation. In the long-term, engaging the public in such a manner could encourage them to pursue further ownership over their data trail, and as a result, seek the creation of a legal framework that the markets and our society sorely lack.