Privacy and Digital Mosaics: Lessons from Pollution Control

E. Susanna Cahn
Lubin School of Business, Department of Management & Management Science
Pace University

Victor Glass
Center for Research in Regulated Industries and Department of Finance and Economics
Rutgers Business School

Contact: ecahn@pace.edu

Abstract

Digital Mosaic Pollution (DMP) arises when bits of information originally gathered for other purposes escape their original boundaries. The metaphor of a mosaic implies that bits of information, each not valuable by itself, when pieced together can create a clear, or distorted, picture of a person, depending on the collector's aims. The pollution metaphor explains how the effluent data becomes available for other purposes, including unintended and unwanted aggregation into personal digital mosaics, without consent or even awareness. Privacy invasion is an unwelcome byproduct. Much like pollution, unwanted data exposures are difficult or impossible to make private again. To gauge societal damage from information pollution, we consider privacy from a variety of academic perspectives: ethics, economics, law and regulation. The pollution analogy focuses regulatory policy and legal strategies for protecting privacy on the creators of Digital Mosaic Pollution where it can be most efficient and effective.

Keywords: digital mosaic, pollution, sustainability, information privacy, data privacy

Introduction

Privacy is important, so important that when there is a loss of privacy, it is called an *invasion* of privacy. People value privacy, but it is hard to put a monetary value on it. Privacy is variously defined as a moral right, control over access to personal information, protection against intrusion, disclosure, and appropriation. The importance of privacy calls for effective legal protection. Yet ambiguous understandings of just what privacy is, make it difficult to craft effective, acceptable privacy policy.

Traditionally, privacy was associated with physical items. The home was beyond search and seizure without a warrant. Sensitive personal information such as health records were typically held by a single doctor on physical records that could be destroyed. Now the home is less a sanctuary than a base station for transmitting and receiving data, and health care records are online, often traded among health care agencies. The Internet and related developments in cloud storage and artificial intelligence associated with data mining have created a gulf between traditional views of privacy and online privacy. In effect, the information age is rapidly supplanting the age of

tangibles. Rengel (2013) surveys the many ways in which technology enables invasion of privacy. The transition is upending cultural norms. As a result, law and regulation are in catchup mode.

This paper reviews various understandings of privacy by ethics, economics, and law. Then it considers how digital mosaics can be created from bits of separately collected digital information. A new perspective is added to the mix by analogy to environmental pollution. Digital Mosaic Pollution (DMP) is a metaphor which adds to understanding the nature of privacy.

Digital Mosaic Pollution is an appropriate metaphor for private information that escapes boundaries in a digital world; it conjures images created from bytes of data that travel across a digital landscape. Digital Mosaic Pollution is an effective policy metaphor because it represents a pervasive atmosphere of potential privacy invasion that follows from unwanted byproducts of trading personal information. The pollution metaphor helps productively focus regulatory and legal strategies that strengthen information privacy with the aim of improving social welfare. This metaphor is most appropriate for developing privacy protection policies for online data aimed at private institutions and government agencies that release or market personal data.

This paper is organized as follows: Section 1 summarizes academic perspectives on privacy from ethics and economics as well as regulatory and legal approaches to protect privacy. Section 2 describes the development of digital mosaic theory. Section 3 uses analogy to environmental pollution to characterize Digital Mosaic Pollution - escaped digital information that can be recycled into digital mosaics for online privacy invasions. Section 4 recommends methods for abating this type of pollution. Section 5 contains concluding statements.

Section 1: Perspectives on Privacy

Before discussing policy, we consider privacy from three academic perspectives: from those used by ethicists, economists, and jurists because each group has developed its own set of remedies for privacy invasion based on their own perspective and set of values.

Ethics: The Right to be Left Alone

Ethicists see privacy as a moral right. Often quoted as the origin of the modern representation of privacy is “the right of the individual to be let alone” (Warren & Brandeis, 1890). Bloustein champions privacy as a moral value by emphasizing the critical importance of privacy to individual freedom, independence, dignity and integrity (1964). More specifically, privacy may be seen as control over personal information, or as restricted access to personal space. It protects "the right of determining…to what extent his thoughts, sentiments, and emotions shall be communicated to others” (Warren & Brandeis, 1890).

Rachels (1975) connects privacy with control. People behave differently in different social situations and share information differently in different relationships. Privacy rights allow people to manage their human relationships by controlling who has access to what information about themselves. In this sense, privacy is an aspect of liberty because it allows us to choose our relationships. Parent (1983) echoes the connection of privacy with control, including though not limited to control over information about oneself. Moor (1990) makes the case that normatively private situations (those with moral or legal restrictions on access rather than “naturally” private) are culturally determined. He argues that privacy is intrinsically valuable as well as being necessary to develop social relationships and for autonomous decision making.

In many situations, not limited to "private places," privacy rights are violated if one is observed without consent. Yet even the concept of consent is nuanced. Moore (2000) differentiates between thin consent and thick consent. If an employee is notified that they must consent to workplace surveillance in order to maintain employment and the employee concurs because the alternative is onerous, that is "thin consent" (p. 701). Where jobs are readily available and the employee in question does not need the job or can easily find another job, consent to the same notification would be considered "thick consent" (Moore, 2000, p. 702). His criticism of technology-enabled routine monitoring of employees is that "even if such monitoring somehow produced an overall net increase in utility, it would still be unjustifiable" because it violates privacy (Moore, 2000, p. 707). Wall (2011) extended the need for consent to information privacy, defining privacy as "the moral right to consent to access by others to one's personal information" (p. 69).

The ethical perspective suggests that loss of privacy is a personal loss regardless of whether it has market value as a tradable good. Even when a cost-benefit analysis justifies erosion of privacy, there is still an intrinsic loss.

Economics: The Value of Privacy

Economists treat privacy as both a source of market imperfections and exploitation, as well as a source of protection from personal exploitation. Classical economic models do not easily account for the value of privacy as a source of personal utility because it is not a specific product in the usual sense.

In classical economics, the basic competitive economic model shows that full-disclosure and voluntary trade maximize consumer welfare and producer surplus. Both sides gain from voluntary trade despite acting for their own gain. This model rests on stringent assumptions associated with "Economic Man." This person knows his/her preferences, knows product characteristics, and knows the alternatives available. Economic Man's choices are the outcome of a highly rational decision process. In this rarified model, privacy is irrelevant because everyone knows everything.

In actuality, traders do not have perfect information. Personal information has value when the holder of the information can strike a more satisfying or profitable trade. Many market failures examined by economists are associated with incomplete information or asymmetric holding of information. The famous Market for Lemons article (Ackerloff, 1970) explains that used cars sell at a deep discount because potential buyers assume the used car is a lemon; otherwise, why sell it? Insurance companies need to set rates to uncover customers who are likely to have health problems. People who are insured may be more reckless (the Moral Hazard Problem). Workers and managers may shirk their responsibilities or put their own personal benefits ahead of the company's requirements (Baye & Prince, 2017, Chapter 6). To overcome problems associated with incomplete information, parties sometimes engage in lengthy negotiations, and develop formal contracts with contingency clauses to limit opportunistic behavior. Sometimes business-to-business buyers and sellers with regular important and complex trades will choose to merge their two companies so as to share information and manage more operations in-house. Such mergers unify goals, reduce transaction costs, and reduce market risk (Gaughan, 2013, p. 226).

Another key assumption of the basic economic model is secure and known property rights, including the right to retain or transfer that property. Incomplete property rights associated with

personal information lead to a form of "commons"[1] exploitation. The problem of overuse of common pasture is a classic example. Cattle grazers overuse public land because each myopically assumes that the best strategy is to feed as much grass as possible to his own cattle. The pollution problem is associated with "free" air. The cost of pollution drifts over other peoples' property. Insecure property rights potentially harm market dynamics. The commons problem associated with personal information occurs because it is not alienable like a traditional product. One cannot sell one's social security number to someone else and allow that person or entity to masquerade as you. Having an incomplete property right means the person always has an interest in the released personal information. Its use by others can produce personal harm. For example, trading personal information raises the probability of identity theft.

Another difficulty is that personal information is not a single product. It covers a range of data types from intimate to normally exposed, such as being in a public space. In the basic economic model, market trades involve distinct products with known characteristics and known uses. Even if one could define digital property rights, the value of personal information will vary depending on who uses it and how it combines with other pieces of personal information. The values of these connections are often unknown. At a minimum, this raises the issue of the high cost of contracting to sell personal information. A person would need to settle on a price for personal information with every entity that he or she voluntarily offers information to in exchange for services.

The cost of contracting increases when one recognizes that the market for personal information is itself not transparent. Sometimes people want to control their own data, not to keep it secret, but to profit by selling it themselves rather than leaving data collection to an intermediary cloud business (Mawad et al., 2018). While personal data is widely traded commercially, consumers have not been generally aware of third party transactions or even whether their data is being collected, making the contracting problem even more unrealistic (Acquisti & Wagman, 2016). Firms hardly known to the public collect, analyze and trade huge datasets containing information on many, many individuals (Patrizio, 2020; Marr, 2016).

Companies often barter services for personal information, which eliminates the pricing mechanism as a means of valuing personal information. Google, for example, gathers transaction data and can observe personal movements if one uses Google Maps for driving directions. Companies enhance the value of bartered personal information by aggregating across people and developing useful databases and algorithms for uncovering market patterns. These companies expect a return on their investments in "free" applications, but the value is not posted.

Referring to Google or to Amazon raises the question of effects of market concentration on the value of personal information. Information rich online companies have an indirect peek at someone's information because they have similar data from other people who have volunteered data. Even in the case where a large online platform had to pay people for use of personal information, they would be at a tremendous competitive advantage for setting prices for data. In Amazon's case, especially, antitrust advocates like Khan (2016) believe that the company exploits users of their platform by seeing theirs and other comparable transactions.

---

[1] Where many have common or shared access to use the same resources and one cannot easily exclude others from exploiting the resource *Digital Library of the Commons dlc.dlib.indiana.edu*

As opposed to classical economists who focus on the problems associated with privacy, a new group of behavioral economists believe that privacy is a protection against "nudging" exploitation. Even as the Economic Man model took hold in the economics profession in the early 20th century, notable economists such as Frank Knight had serious issues with it. His ideas are a bridge to the behavioral economists who present another economic view for the value of privacy. Knight believed that economics must consider values beyond the value of trades. The Economic Man model suggests that this rational man's behavior is perfectly predictable if you know his utility function and budget constraint. While the model is useful for explaining why demand increases when prices decline, Knight said it should not mask the obvious that human behavior is often impulsive and unstable, and marked by partially thought out decisions.

From Knight's perspective, a person's "wants" are not fixed. They are the product of upbringing and aspirations. Wants are generated by looking forward and higher. Life is not striving for ends but mainly striving in a certain direction. True achievement is an elevation of desire, a cultivation of tastes, and an exploration of values. People sacrifice for a better life worthy of respect. Choices define self. Work is meaningful because it also defines one's capabilities. People desire to be like others but also want to be different (Knight, 1935, p. 43). His perspective is that man is as much a "romantic animal" as a rational animal. People cover themselves with clothes and misrepresent their intellectual, emotional, and moral nature in language and behavior. These deceits and concealments are not necessarily bad, according to Knight. By posing as better than one is, the pretense becomes habit, and improves character (Knight, 1947, pp. 405-409). Economists have not explored as far as we know the value of pretenses on expectations and future activities that would be undermined by exposure of personal information. Instead, the focus is on whether past mistakes such as committing a crime should not appear on a background check if it occurred long ago. The debate is in terms of market efficiency. Employers may overreact to this type of information.

Behavioral economists have recently focused on the effects of human frailties on transactions. Their experiments show that behavior is systematically biased. People over-react to data. They have a myopic view of how long they will actually live. They can be manipulated during psychologically vulnerable periods. Artificial intelligence techniques can encourage impulsive buying and over-reactions to political events (Thaler, 2018).

By contrast, mainstream economics typically assumes that more shared transaction information available to the market improves market efficiency, and as a result, is wealth enhancing. While this may be true in the aggregate, shared information can change the allocation of benefits because of distortions caused by superficial data. For example, data on a person's race or gender could potentially be used for price discrimination (Elliott, 2016).

The economic perspective on the value of privacy (or personal information) centers on who, or which organization, can retain property rights for using or trading private information. In the real world, private information has economic value. Lack of transparency, incomplete property rights, opaque pricing, and large information aggregators all play a role in who benefits from the economic value of private information.

Law and Regulation: Protecting Privacy

The legal system aims to protect an intrinsic right to privacy and to compensate for value lost from privacy invasions after they have occurred. Thus, law incorporates concepts from both

ethics and economics. A body of legal precedents have developed to define privacy, breaches of privacy, and remedies. The perspective of Warren and Brandeis (1890), which presented privacy as a right unto itself, supports the notion that the legal system should make an explicit commitment to the value of privacy. Laws should protect privacy and judicial remedies should recognize the undesirability of privacy losses (Gavison, 1980). Bloustein (1964) states that "the historical development in the courts of the concept of privacy stems from and is almost exclusively devoted to the quest for such a civil remedy" (p. 964).

Initially privacy law emphasized physical invasions of privacy, freedom of access or prevention from access.

> [Privacy]… is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. This concept of privacy as a concern for limited accessibility enables us to identify when losses of privacy occur (Schauer, 2001, p. 423).

Functionally, law looks at what is actionable, that is, cases where the damaged party can sue. Privacy law has evolved from legal protection of photographs disseminated without consent, foreshadowing the subsequent applications of privacy law to information privacy. Privacy law sees privacy as a concept of freedom of choice. Individuals may choose with whom they share their space and their information. The basic principle that emerged is that protection of privacy promotes liberty, autonomy, selfhood, and human relations, and furthers the existence of a free society (Schauer, 2001).

Much of privacy case law relies on the Fourth Amendment to the U.S. Constitution which protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" (*U.S. Constitution*. Amend. IV). "The Fourth Amendment has been interpreted in court as forbidding "every search that is unreasonable and is construed to safeguard the right of privacy" (*United States v. Lefkowitz*, 1932). Addressing the difficulty of determining what constitutes a breach of privacy needing remedy, a societally based standard is the "reasonable expectation" of privacy (*Katz v. United States*, 1967).

In contrast to the widely held view that privacy is a right unto itself, Prosser asserted that privacy simply overlaps four tort interests: intrusion into private affairs, public disclosure of embarrassing facts, putting persons in a false light, appropriation of name or likeness (Prosser, 1960, p. 389).

Economic theory has influenced legal thinking in recent decades. Richard Posner (1981) pointed out that the economic efficiency standard for the law is not ethically neutral. The common law and economic theory have roughly similar ethical standards -- people have basic rights that must economic approach to privacy law is that effective laws promote market efficiency, and as a result, are wealth enhancing. In general, laws should be enacted when the expected reduction in losses is larger than the burden of compliance.[2] Gordon demonstrates that this is true for the risk of cybersecurity breaches. Moreover, the liability should fall on the party most responsible for an accident or personal injury (Gordon et al. 2015).

---

[2] See Learned Hand Test in C. Veljanovski, *2007. Economic Principles of Law. Cambridge, UK: Cambridge University Press.*), 186-190.

Often, technology is involved in various privacy problems, as it facilitates the gathering, processing, and dissemination of information. Privacy problems, however, are caused not by technology alone, but primarily through activities of people, businesses, and the government. The way to address privacy problems is to regulate these activities (Solove, 2006).

The complement to legal ex-post remedies for privacy invasion are regulations– ex-ante positive rules – that define acceptable behavior. These rules have their legal basis in legislation. For example, the Federal Trade Commission (FTC) is one of the leading regulatory bodies that focuses on commercial privacy.[3] The FTC summarizes the elements of Fair Information Practices as five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress (Federal Trade Commission, 1998, p. 7). The FTC is one among many agencies that regulate privacy practices. Other regulatory agencies have jurisdiction to protect individual health care, education, financial, employment and other records (Office of the National Coordinator for Health Information Technology, 2010). Regulatory agencies can impose fines for noncompliance and refer certain cases to the judicial system in cases of criminal activity.

Whether done through legal precedents, regulations, or legislation, extending privacy rights to information is difficult because of the variety of personal data being gathered and processed. The reasonable expectation of privacy might be violated by any of four basic groups of potentially harmful activities: (1) information collection, (2) information processing, including aggregation and secondary use and failure to inform the data subject (3) information dissemination, and (4) invasion, interfering in the individual's decisions (Solove, 2006, p. 488).

Another facet of privacy protection is the nature of the information – intimate, sensitive, or confidential information is private with respect to collection and dissemination. Nissenbaum (2004) reiterates the traditional notion of private places. Also, who is the information collector—government or a private entity. Nissenbaum (2004) introduces the concept of 'contextual integrity' as an important consideration to protect individuals against invasion of privacy. She argues that there are norms of information gathering everywhere that are appropriate by context, even in public places. If those norms are violated, there is an invasion of privacy. She particularly notes that power asymmetries, as when there is systematic widespread government surveillance of private individuals, need to be guarded against.

The European Union (EU) has detailed systematic rules for privacy protection spelled out by the General Data Protection Regulation (European Parliament, Council of the European Union, 2016) whereas in the US such regulation is on a case-by-case basis developed by the FTC. In effect, the EU rules are setting a universal standard as they apply to any organization anywhere

[3] The Federal Trade Commission (FTC or Commission) is an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. This broad authority allows the Commission to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models. (https://www.ftc.gov/reports/privacy-data-security-update-2016)

that collects data from EU citizens. Proposals have been made for a more rules-based approach in the US (United States Government Accountability Office, 2019). As communication and trade are global, efficient privacy rules need to be global as well.

Section 2: Digital Mosaics

The mosaic as a metaphor for aggregating bits of information has found its way into the legal system. In Halkin vs. Helms, the court rules that "[I]ntelligence gathering in this age of computer technology is more akin to the construction of a mosaic than it is to the management of a cloak and dagger affair" (*Halkin v. Helms*, 1978). This statement was prescient because in 1978 the internet and cellular service were not available to the public. Government was tapping phones to eavesdrop on conversations. Once the digital revolution began, mountains of personal information became available. Computer analysis, especially, of data patterns, could then piece together seemingly insignificant bits of information to create a meaningful picture (Patel & Goitein, 2015, p. 19). Even if each information leak appears harmless, the mosaic creates costs and benefits (Pozen, 2005). Even when all the pieces of information are already publicly available, aggregation can still cause problems (Solove, 2006, p. 559).

Pozen (2005) traces the history of the mosaic theory back to 1972 (p. 632). The mosaic theory was articulated by the Navy as a counterargument to shield information from disclosure under the freedom of information act. A series of court cases argued pros and cons of how the mosaic theory could be used to balance the effect of information-gathering technology (*United States v. Marchetti*, 1972; *Halkin v. Helms*, 1978; *Halperin v. CIA*, 1980; *CIA v. Sims* 1985). After 9/11 the mosaic argument was used even more aggressively to shield government information from public view.

Another variation on the use of the mosaic theory was to protect individuals against warrantless searches where the aggregation of information taken from individual instances, each not in itself requiring a warrant, could be taken together to provide incriminating evidence. The idea (though not the term) was introduced in several cases (*United States v. Maynard*, 2010); *United States v. Jones*, 2012). Arguments in these cases discuss the impact of information aggregating on what constitutes a search, where the details involve electronic surveillance over a period of time. Kerr suggests that a mosaic theory argument is put forward to restore the balance of power upset by changes in technology. "The mosaic theory attempts to restore the balance of power by disabling the government's ability to rely on what computerization enables" (Kerr, 2012, p. 345).

Online data blurs the distinction between confidentiality and anonymity. Confidential information is known and/or recorded, but concealed. Confidentiality may be created by a locked door or by an algorithm. Security of confidential information is a never-ending series of protective and deciphering devices. However, locks may be picked and algorithms may be decoded or hacked, so that confidentiality cannot be guaranteed to be permanent. Duncan and Whittington (2015) remind us that "the threat environment…is not static… As soon as a new vulnerability is found, software developers race to find a solution. As soon as patches are released, the bad guys race to counter the patch. And so the vicious circle continues" (p. 525). Anonymous information is missing some identifying bits of data; not simply hidden but actually not known. Yet, the mosaic theory suggests that even anonymous information may be deciphered if enough of the available bits can be assembled.

Section 3: Digital Mosaic Pollution

Digital Mosaic Pollution arises when bits of information originally gathered for other purposes escape their original boundaries. The effluent data becomes available for other purposes, including unintended and unwanted aggregation into personal digital mosaics, without consent or even awareness. Digital Mosaic Pollution is a negative externality. These unwanted mosaics have economic value to businesses or political value to the government, but are produced through questionable ethics with potentially negative consequences to the individuals whose information it was. The pollution metaphor creates a meaningful picture of the fragile nature of privacy and irretrievability of its loss. Digital Mosaic Pollution invokes images of digital processing plants building images from shards of personal information sold, received, or stolen. The constantly updated "recommended for you" list on YouTube is an obvious example of tracking personal viewing habits. This unnerving oversight is like walking alone at night to purchase something. There is a nagging probability of becoming a victim, in this case of identity theft.

Earlier use of metaphors illuminated how government or huge institutions can control people by invading their privacy. Solove (2001) references Big Brother and Kafka to conjure an unseen, pervasive voyeur with power to control personal behavior. Similarly, Moore (2000) references Bentham's transparent workhouse as a metaphor. Bentham (1843) conceived of a Panopticon, a prison designed so that the inmates would not know when they were being watched; he believed that sense of perhaps always being under surveillance would change their behavior.

A company or government can gather and use seemingly innocuous personal data to develop a personalized mosaic that may range from highly accurate to greatly distorted, but in either case, is a privacy intrusion that makes the public understandably anxious. Damaging exposures can occur now or in the future, that could cripple a person's reputation. The digital pollution can be produced by one company trading personal or even anonymized data with other companies, or by government agencies that collect and release data to the public, such as census data, or collect data surreptitiously and not release it for public viewing.

Complicating the matter, new property rights accrue to organizations that develop and market these digital mosaics. These new property rights have more standing when companies aggregate and anonymize personal data and use it to customize services for particular consumer market segments.

The pollution metaphor conjures the real privacy threat of data escaping its original intended use and floating through the ether to unknown databases, where it is almost impossible to retrieve and to erase. The one-way nature of information exposure is very similar to environmental pollution. It is often exposed as a byproduct of some other activity; thus it can be seen as an economic externality. Once exposed, it is difficult and expensive, if not impossible to control and make private again.

Digital Mosaic Pollution is a somewhat weaker metaphor for police and national security invasions of privacy but still apt. Agencies such as such as the National Security Agency (NSA) gather masses of data on people living in the United States to develop mosaics of people to identify foreign agents of malignant foreign powers. As a byproduct, NSA can construct digital mosaics for people not the target of the investigation (Goitein & Patel, 2015, p. 34). Unchecked surveillance can poison a nation's cultural atmosphere. The Fourth Amendment was meant to protect people from government invasions that would poison the notion of personal freedom. The

home, especially, was protected from search and seizure without a search warrant. The interpretation of the Fourth Amendment has been extended to personal information that one should expect to remain private. Now cell phones may be the equivalent of the home as a repository of sensitive personal history. Monitoring devices may invade personal space without physical entry. National security agencies can gather personal information and refuse to release it because some outside entity may be able to use artificial intelligence to reconstruct government surveillance policies.

Controlling information pollution among private institutions is similar in aim to enforcing cybersecurity, which is a feature of corporate social responsibility. It is in the firm's long term sustainability interest, as well as part of their social contract to safeguard the information of their customers and the public. Shackelford, Fort, and Charoen (2016) apply lessons from the green movement to corporate sustainability. Their argument stems from treatment of cyberspace as a commons, or a common pool of exhaustible resources. Overuse, a feature of what we here call digital pollution, might occur when spam messages consume limited bandwidth (pp. 1999-2001). A similar argument is made about physical outer space as a commons with space debris as an externality (Shackelford, 2014).

Gordon, et al. (2015) makes the case, though, that it is not in a private firm's financial interest to invest sufficiently in cybersecurity to cover its full cost, much less the total social cost to both the firm and to outside stakeholders who are at risk. This is another externality argument, akin to the disincentive for private firms to pay the full cost of environmental cleanup. Absent strong environmental policy, it is not in a private firm's financial interest to invest in pollution abatement because the costs are largely externalities. As a derivative, there will be underinvestment in environmentally beneficial technology. "A firm that invests in or implements a new technology typically creates benefits for others while incurring all the costs. The firm therefore lacks the incentive to increase those benefits by investing in technology" (Jaffe, Newell & Stavins, 2005, p. 166). A parallel argument can be made regarding private investment in protecting privacy. Without pressure from public policy, it is not in a private firm's financial interest to pay the full cost to abate Digital Mosaic Pollution.

Section 4: Strategy for Defining and Abating Digital Mosaic Pollution

Digital Mosaic Pollution suggests a harm to society. The harm is not easily identified with an individual victim in quantifiable ways. The market has not solved the pollution problem because of the difficulty with ill-defined personal information property rights. Complete transfer of personal information such as a social security number is impossible. In the online economy, many transfers occur routinely, and different transactions have overlapping transfers of data, making online contracting with individuals costly. Avery Katz (1990) cites implementation costs and strategic behavior as reasons why the market will not produce efficient privacy solutions on its own. Implementation costs include the cost of executing, administering, and enforcing privacy agreements. Strategic behavior leads bargainers to maximize their own gain at the expense of the other party (Sheldrake, 1999, p. 1083). Third-party "privacy seals of approval" such as TRUSTe require adherence to certain minimum standards in areas such as notice of information practices and consumer choice regarding secondary uses (Killingsworth, 1999, p. 65). Unfortunately, such attempts have failed (TrustArc, 2021). In this type of environment, government can act to institute rules that improve market efficiency and protect the intrinsic values associated with privacy.

Despite the difficulty, public policy should address the problem. A starting point is to define Digital Mosaic Pollution more concretely. The first stage is to identify sources of pollution and whether the pollutants themselves are dangerous. The Federal Communications Commission has defined personally identifiable information (PII) as the most sensitive category. It includes a person's social security number, date of birth, and other personal information permanently connected to an individual. A second tier of personal information is customer proprietary network information (CPNI) and its extension to Internet transactions. CPNI as a broad category includes information about a person's communication records (FCC, 2016). Other categories of personal information can be developed to identify more possible and future sources of pollutants. Consideration should also be given to the risk of enabling a digital mosaic.

The second stage is to identify the polluters. The polluters under consideration here are private institutions that in socially damaging ways gather, process, use, store, or trade personal information, even if anonymized. The main culprits are firms that treat data as a marketable service and online companies with poor data security practices. These private sector organizations are the primary sources of Digital Mosaic Pollution and the major targets of malicious privacy invasion. Unlike customers who access many websites and have an imperfect knowledge of the data collected from them or their use, companies are much more aware of the risks associated with their internal databases. These databases are critical to companies being competitive in the online economy. Their comparative awareness of privacy risks motivates the focus of privacy pollution control on data gathering organizations. Strategies for maximizing the social benefits of privacy welfare should focus regulatory and legal reforms on business-to-business exchanges of data and lax internal security that generate Digital Mosaic Pollution.

Although the online economy is young, there is enough history to form digital mosaics of the polluters themselves. In commerce, companies like Target, Facebook, and Yahoo have experienced enormous data breaches, but they are not the only ones. Verizon tracks the history of data breaches and shows they are extensive (Verizon, 2021). Beyond data breaches are losses of privacy that are uncomfortable even if harmless. For example, "recommended for you" marketing strategies based on data mining of large datasets seem like "big brother" is monitoring your habits. The availability of GPS data and other tracking information can identify people with great accuracy because people are creatures of habit. Even anonymized data can be re-identified. Based on only three bits of information: gender, date of birth, and zip code, 87% of the population of the United States is uniquely identifiable (Sweeney, 2000).

Data miners have a fiduciary responsibility to maintain personal privacy. They could be held personally liable for unwanted data mosaics and data breaches. Monitoring products such as GPS could be limited in clarity to avoid privacy invasions. For example, aerial pictures should not contain sensitive personal information. Data gatherers such as Yahoo or Google are being required to use "best practices" to protect databases. Anonymity rules are being imposed on location-specific and customer-specific data.

Surveys show that people value privacy (Sovern, 1999, p.1057). Giving online consumers the option to Opt-out or better still Opt-in to providing personal information are useful privacy strategies for providing notice. Yet consumers do not exercise those options in numbers representative of their value of privacy for a variety of reasons (Sovern, 1999; Staten & Cate, 2003). So, their practical value is limited because the public does not have the time, inclination, or

competence to assess online privacy statements by corporations.[4] Consumers are unlikely to read or know how to evaluate online terms and conditions, often written in small print. Consistent with the pollution analogy, it is more effective to go after the source instead. Government regulators should set rules for B-2-B transactions and enforce them.

Technical solution to the pollution problem is tricky because technology used to uncover personal data is rapidly advancing. Nonetheless, there are basic market and governmental practices that can limit Digital Mosaic Pollution. Within organizations, database storage, processing, and scrubbing tools can abate pollution. Limiting life of databases can limit long-term threats to personal privacy. Compliance programs that focus on protecting privacy are valuable. Data transmission encryption limits hacking.

Market-based solutions to privacy will help address the problem. However, organizations will mainly focus on their own security issues and still have the incentive to hide or minimize data breaches. The source of a breach may not be obvious at first. For example, Target's data breach was caused by one of its suppliers, HVAC Company. Our belief that the market's response to protecting personal information is incomplete is not meant to suggest that private initiatives won't solve many of the privacy problems. Equipment manufacturers such as Cisco will develop systems for protecting corporate databases. An insurance market is evolving that will encourage companies to adopt good cybersecurity practices. Nonetheless, these market developments will suffer from significant information limitations (Wolff & Lehr, 2017). Beyond that, concentrated attacks by foreign governments may be beyond the capabilities of private enterprises.

Used by governments, website hacking is another attack on privacy with large social consequences. Artificial Intelligence (AI) presents a new form of military attack on property rights (Allen, 2008). Hilary Clinton and Donald Trump have had their lives changed by a form of international cyberterrorism (Democratic National Committee Cyber Attacks, 2021). Again, the source of pollution and the target is an organization, not the individual.

To effectively and efficiently abate Digital Mosaic Pollution, policy-makers need a broad understanding of market-based solutions being developed. For example, Firefox introduced a service that disables third-party cookies by default (Firefox, 2021). Policymakers must also realize that the online economy cuts across many regulatory agencies that were designed to regulate specific industries. A new look at government regulatory structures is necessary.

Legal redress must also be evaluated. The recent Yahoo settlement is instructive. Yahoo was required to pay $85 million in damages for a data breach on 3 billion accounts. There are potentially 200 million who can claim settlement money. Lawyers received $35 million of the total fine (Jones, 2018).

Another possibility that at first seems paradoxical is to improve data sharing among online businesses, security companies, and insurance companies. Using proper controls, governments may improve the efficiency of the cybersecurity market by giving parties a broader view of

[4] Many legislators in the United States would disagree. Twenty-five states are proposing a variety of bills centered on opt-in/opt-out. See Wolak and Halpin (2019). Note that many differing privacy rules will raise the cost of compliance. It may also cause jurisdictional conflicts between the federal and state governments because online traffic is mainly interstate.

cyberattack incidents and actual damages. In a sense, the government would be creating economies of scale for gathering data attack and breach information (Bailey, 2014; Wolff & Lehr, 2017).

The pollution metaphor for digital information leaks suggests regulations to prevent pollution, a pollution tax, and a pollution fund to clean up pollution. Payouts to individuals could follow insurance techniques – premiums netted based on reasonable prevention and potential loss. Tax could be based on expected societal losses from a data breach, ideally paid by the hacker but also by the company holding the data. Note that businesses bear costs of polluting through lower stock prices but that does not cover damages incurred by persons whose private data were exposed. Individuals need legal or regulatory redress.

Remedies for police and national security DMP needs to follow a somewhat different track because it is not the result of data trading market failures. It is a problem of internal controls within government to prevent national security threats or criminal activity from gathering dirt on unsuspecting American citizens for political purposes. Judges and regulators first need to understand public expectations of unwanted search and seizure whether it is by pushing down a door or using a tracking device (Kugler & Strahilevitz, 2016). When it comes to national security, where the cost of making mistakes could be high, and understanding methods for building mosaics complex, judges need experts to determine if classified information is truly sensitive. This will require understanding how mosaics are constructed and if they are plausible in a particular case (Bellovin, et al. 2014). The intent of the Freedom of Information Act (2007) to shed light on the dark corners of public activities where government agents hide their incompetence or law breaking is a key protection of personal freedom. A better understanding of digital mosaic construction will test the boundaries between secrecy that protects national security and openness that protects personal freedom. Proposals for sweeping reform of the Foreign Intelligence Surveillance (FISA) Court process are an active area of legal research (Goitein & Patel, 2015, pp. 45-51).

The pollution metaphor, like other empirically-based guidelines, has the weakness of relying on historical learning, which assumes a level of stability to social processes. As we saw with the financial meltdown in 2008, empirical techniques failed to predict the crash and regulations in place were ill equipped to cope with the crash. The information economy is dynamic and growing. Today's methods for coping with digital pollution will become ineffective if a new virus is developed or quantum computing allows a hacker to decrypt any message. Still the pollution metaphor motivates a new perspective on strategy for reducing and redressing harms of digital mosaics.

Section 5: Conclusion

Digital Mosaic Pollution is a metaphor that captures the intrinsic ethical value of privacy with inherent loss when privacy is invaded. The metaphor captures the economic value that is tempting both private businesses and governments to tap into available data to create informative and profitable mosaics. The pollution metaphor adds a perspective that even seemingly harmless releases of data bits can cause privacy invasions. The metaphor of Digital Mosaic Pollution can be used to guide policy that will inhibit privacy invasion, mitigate data abuses, and redress losses of privacy. The pollution analogy focuses policy on the creators of Digital Mosaic Pollution where it can be most efficient and effective. It helps define new privacy issues, helps organize policy responses already underway, and suggests possible tax strategies to capture the costs of unwanted releases of personal data. Taxes could also be a source of funding to repay people who have

suffered damages associated with privacy invasions. The pollution perspective needs to be developed more fully to target specific but pervasive threats to personal privacy by private institutions.

References

Ackerlof, G. A. (1970). The market for 'lemons': Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics, 84*(3), 488–500.

Allen, J. (2018). AI will change the balance of power. *U.S. Naval Institute, Proceedings 144*(8), 1386. https://www.usni.org/magazines/proceedings/2018-08/ai-will-change-balance-power

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 52*(2), Sloan Foundation Economics Research Paper No. 2580. https://doi.org/10.1257/jel.54.2.442

Bailey, L. (2014). Mitigating moral hazard in cyber-risk insurance. *Journal of Law & Cyber Warfare, 3*(1), 1-42. https://www.jstor.org/stable/26432557

Baye, M. & Prince, J. (2017). *Managerial economics and business strategy*. (9th ed.). McGraw-Hill.

Bellovin, S. M., Hutchins, R. M., Jebara, T., & Zimmeck, S. (2014). When enough is enough: Location tracking, mosaic theory, and machine learning. *New York University Journal of Law & Liberty, 8*, 555–628.

Bentham, J. (1843). *The works of Jeremy Bentham: 39*. *Online Library of Liberty* hosted by Liberty Fund, Inc. http://oll.libertyfund.org/title/222 .

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *New York University Law Review, 39*, 962–1007.

CIA v. Sims, 471 U.S. 159 (1985).

Democratic National Committee Cyber Attacks. (2021, January 27). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Democratic_National_Committee_cyber_attacks&oldid=1003179265

Duncan, B. & Whittington, M. (2015). Information security in the cloud: Should we be using a different approach? In *IEEE 7th International Conference on Cloud Computing Technology and Science*, 523–28. Institute of Electrical and Electronics Engineers.

Elliott, C. (2016, February 5). *Price discrimination isn't only about pink razors*. The Conversation. https://theconversation.com/price-discrimination-isnt-only-about-pink-razors-54132/

European Parliament, Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*. http://data.europa.eu/eli/reg/2016/679/oj

Federal Communications Commission. (2016). Protecting the privacy of broadband and other telecommunications services. Report and Order. WC Docket No. 16-106.

Federal Trade Commission. (1998, June). *Privacy online: A report to Congress*. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

Firefox. (2021, June 4). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Firefox&oldid=1026889602

Freedom of Information Act, 5 U.S.C. § 552 As Amended By Public Law No. 110-175, 121 Stat. 2524 (2007). https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-final.pdf

Gaughan, P. A. (2013). *Maximizing corporate value through mergers and acquisitions: A strategic growth guide.* John Wiley & Sons.

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal, 89*(3), 421–71. doi:10.2307/795891

Gordon, L. A., Loeb, M. P. Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security, 6*(1), 24–30.

Goitein, E. & Patel, F. (2015). *What went wrong with the FISA court?* Brennan Center of Justice. New York University Law School. https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court

Halkin v. Helms, 598 F.2d 1, 8 (D.C. Cir. 1978).

Halperin v. CIA, 629 F.2d 144 (D.C. Cir.1980).

Jaffe, A. B., Newell, R. G., & Stavins, R. N. (2005). A tale of two market failures: Technology and environmental policy. *Ecological Economics, 54*(2–3), 164–74. https://doi.org/10.1016/j.ecolecon.2004.12.027

Jones, M. (2018, October 27). *Yahoo might owe you money in $85 million data breach settlement*. Komando. https://www.komando.com/happening-now/501663/yahoo-might-owe-you-money-in-85-million-data-breach-settlement

Katz, A. (1990). The strategic structure of offer and acceptance: Game theory and the law of contract formation, 89 *Mich. L. Rev.* 215, 225, 255. In Jeff Sovern (1999), Opting in, opting out, or no options at all: The fight for control of personal information. 74 *Wash. L. Rev.* 1033, 1083.

Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).

Kerr, O. (2012). The mosaic theory of the Fourth Amendment. *Michigan Law Review, 111*, 311–54.

Khan, L. M. (2016). Amazon's antitrust paradox. *The Yale Law Journal, 126.* http://digitalcommons.law.yale.edu/ylj/vol126/iss3/3.

Killingsworth, S. (1999). Minding your own business: Privacy policies in principle and in practice. *Journal of Intellectual Property Law*, 7(1, Fall), 57–98.

Knight, F. H. (1935). *The ethics of competition*. The University of Chicago Press.

Knight, F. H. (1947). *Freedom and reform*. Harper & Brothers.

Kugler, M. B. & Strahilevitz, L. J. (2016). Actual expectations of privacy, fourth amendment doctrine, and the mosaic theory. *The Supreme Court Review, 2015*(1), 205–63. https://doi.org/10.1086/686204

Marr, B. (2016, February 12). *Big Data: 33 brilliant and free data sources anyone can use*. Forbes. https://www.forbes.com/sites/bernardmarr/2016/02/12/big-data-35-brilliant-and-free-data-sources-for-2016/#4ac8b44fb54d

Mawad, M., Fouquet, H., Grant, N., & Li, D. (2018, June 7). *Scared by Facebook? Wait till millennials are selling their data.* Bloomberg Technology. https://www.bloomberg.com/news/articles/2018-06-08/scared-by-facebook-wait-till-millennials-are-selling-their-data

Moor, J. H. (1990). The ethics of privacy protection. *Library Trends 39*(1-2 Summer & Fall), 69–82.

Moore, A. D. (2000). Employee monitoring and computer technology: Evaluative surveillance v. privacy. *Business Ethics Quarterly 10*(3), 697-709.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review 79*, 119–58. https://doi.org/10.1525/sp.2007.54.1.23

Office of the National Coordinator for Health Information Technology. (2010, February 18). *Summary of Selected Federal Laws and Regulations Addressing Confidentiality, Privacy and Security*. https://www.healthit.gov/sites/default/files/federal_privacy_laws_table_2_26_10_final_0.pdf

Parent, W. A. (1983). Privacy, morality, and the law. *Philosophy & Public Affairs, 12*(4), 269–88.

Patel, F. & Goiten, E. (2015). What went wrong with the FISA court. Brennan Center for Justice. New York University School of Law.

Patrizio, A. (2020, November 13). *Top big data companies*. Datamation. https://www.datamation.com/big-data/big-data-companies.html

Posner, R. (1981). *The economics of justice*. Harvard University Press.

Pozen, D. E. (2005). The mosaic theory, national security, and the Freedom of Information Act. *Yale Law Journal, 115*, 628–79.

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383–423.

Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs, 4*(4 Summer), 323–33. http://www.jstor.org/stable/2265077

Rengel, A. (2013). Privacy-invading technologies and recommendations for designing a better future for privacy rights. *Intercultural Human Rights Law Review, 8*, 177–230.

Schauer, F. (2001). Introduction : The legal construction of privacy. *Social Research, 68*(1), 51–53.

Shackelford, S. J., Fort, T. L., & Charoen, D. (2016). Sustainable cybersecurity: Applying lessons from the green movement to managing cyber attacks. *University Of Illinois Law Review, 2016*(5), 1995–2032. https://doi.org/10.2139/ssrn.2324620

Shackelford, S. J. (2014). Governing the final frontier: A polycentric approach to managing space weaponization and debris. *American Business Law Journal, 51*(2 Summer), 429–513.

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53*, 1393–1462.

Solove, D. (2004). *The Digital Person*. New York University Press.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560. https://doi.org/10.2307/40041279

Sovern, J. (1999). Opting in, opting out, or no options at all: The fight for control of personal information. *Washington Law Review, 74*, 1033.

Staten, M. E. & Cate, F. H. (2003). The impact of opt-in privacy rules on retail credit markets: A case study of MBNA. *Duke Law Journal, 52*(4, February), 745–786.

Sweeney, L. (2000). Simple demographics often identify people uniquely. Pittsburgh: Carnegie Mellon University, Data Privacy Working Paper 3. https://dataprivacylab.org/projects/identifiability/paper1.pdf

Thaler, R. H. (2018). From cashews to nudges: The evolution of behavioral economics. *American Economic Review, 108*(6), 1265–87.

TrustArc. (2021, May 16). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=TrustArc&oldid=1023375094

U.S. Constitution. Amend. IV. https://constitution.congress.gov/constitution/amendment-4/#amendment-4

United States Government Accountability Office. (2019). *Internet privacy: Additional federal authority could enhance consumer protection and provide flexibility* (GAO-19-52). Report to the Chairman, Committee on Energy and Commerce, House of Representatives. https://www.gao.gov/products/gao-19-52

United States v. Jones, 132 S. Ct. 945 (2012).

United States v. Lefkowitz, 285 U.S. 452, 464 (1932).

United States v. Marchetti, 466 F.2d 1309 (4th Cir. 1972).

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

Veljanovski, C. (2007). *Economic principles of law*. Cambridge University Press.

Verizon. (2021). *Data breach investigations report.* https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf?_ga=2.86484828.570452981.1623173480-531269994.1623173480

Wall, F. & Greiling, D. (2011). Accounting information for managerial decision-making in shareholder management versus stakeholder management. *Review of Managerial Science*, 5, 91–135. https://doi.org/10.1007/s11846-011-0063-8

Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5 (Dec. 15), 193–220.

Wolak, J. T. & Halpin, J. (2019). New data privacy and security laws will impose strict mandates on businesses. New Jersey Law Journal. Law.com https://www.law.com/njlawjournal/2019/11/25/new-data-privacy-and-security-laws-will-impose-strict-mandates-on-businesses/

Wolff, J. & Lehr, W. (2017). Degrees of ignorance about the costs of data breaches: What policymakers can and can't do about the lack of good empirical data. http://dx.doi.org/10.2139/ssrn.2943867