Minnesota Journal of Law, Science & Technology

Volume 18 | Issue 2 Article 2

June 2017

The Dynamic Effect of Information Privacy Law

Ignacio Cofone
Yale Law School

The Dynamic Effect of Information Privacy Law

Ignacio N. Cofone*

ABSTRACT

Discussions of information privacy typically rely on the idea that there is a tradeoff between privacy and availability of information. But privacy, under some circumstances, can lead to creation of more information. In this article, I identify such circumstances by exploring the ex ante *incentives created by entitlements to personal data and evaluating the long-term effects of privacy. In so doing, I introduce an economic justification of information privacy law.*

Under the standard law & economics account, as long as property rights are defined and transaction costs are low, initial right allocations should be irrelevant for social welfare. But initial allocations matter when either of these two conditions is absent. Allocations also matter for production of goods that do not yet exist. Personal information has these characteristics. While the costs of disseminating information are low, transaction costs to transfer an entitlement over it are not. In addition, availability of information requires disclosure—and thereby imposes costs. This analysis challenges the traditional economic objection to information privacy and provides a new justification for privacy rules by casting them as entitlements over personal information.

The approach I develop here provides a framework to identify which types of information ought to be protected and how privacy law should protect them. To do so, it analyzes the placement and

---

* J.S.D. candidate and Resident Fellow, Yale Law School, Information Society Project. Contact: *ignacio.cofone@yale.edu*. Many thanks to BJ Ard, Bertrand Crettez, Klaus Heine, Al Klevorick, Jake Miller, Stephan Michel, Rosa Po, Bibi Van den Bergh, Ann-Sophie Vandenberghe, and Ari Waldman for their invaluable comments to earlier drafts. I am also grateful to the participants of the Internet Law Works in Progress Conference (New York, 2016) for their useful feedback.

optimal protection of personal information entitlements while also examining the commonalities between information privacy and intellectual property. At a more abstract level, it sheds light on the desirability of a sectoral versus an omnibus information privacy law.

INTRODUCTION

While the Internet's technological characteristics, to some extent, offer privacy with no precedents,[1] they also produce a loss of privacy with no precedents. For example, our browsing

1. In social interactions people know our face, gender, general physical characteristics, and can have a good guess at our weight and age. On the Internet, on the other hand, we can access information that we would be embarrassed to look for in a library, or shop for any item that we would not like to be seen buying in a shopping mall. On the Internet, fellow shoppers do not know our particular identity and potential members of our community do not know which information we are accessing.

patterns can be known by Internet service and content providers, as well as third parties, with a wide array of technological developments such as cookies and fingerprinting. In addition, people anywhere in the world can learn personal information about us with just a few searches.

In particular, two changes that affect the incentives in privacy exchanges took place in the last decade. The first is big data, which makes surveillance significantly easier for both public and private parties.[2] The second is the decentralization of how the Internet's content is generated. Both modifications imply that technology changed the context in which privacy-related interactions take place and, consequently, that the desirable scope of privacy protection might have changed as well.

Regarding the first change, advancements in search algorithms that reduce the cost of information retrieval facilitated the accessibility of information. Their development was paired with increasing storage capacities and a reduction in storage costs that increase the durability of information.[3] As a result, information about people's lives is increasingly recorded and stored in an accessible way. This makes personal information more vulnerable to third parties—both public and private—and increases the repercussions of people's actions.[4] This vulnerability can reduce well-being by producing discomfort, and can create chilling effects on behavior that

---

2. Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1913–15 (2013); James Grimmelmann, *Big Data's Other Privacy Problem*, *in* BIG DATA, BIG CHALLENGES FOR EVIDENCE-BASED POLICY MAKING 211 (Kumar Jayasuria & Kathryn Ritcheske eds., West Acad. 2015); *see also* Omer Tene & Jules Polonetsky, *Privacy In The Age Of Big Data: A Time For Big Decision*, 64 STAN. L. REV. ONLINE 63, 65 (2012) ("The harvesting of large data sets . . . rais[es] concerns about profiling, discrimination, exclusion, and loss of control.").

3. David S.H. Rosenthal et al., *The Economics of Long-Term Digital Storage*, *in* MEMORY OF THE WORLD IN THE DIGITAL AGE: DIGITIZATION AND PRESERVATION 513 (2012) (explaining that the cost of storing digital media has dropped exponentially in the last thirty years); JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 186 (2008), http://futureoftheInternet.org/download/ ("[N]early all formerly transient communication ends up permanently and accessibly stored in the hands of third parties, and subject to comparatively weak statutory and constitutional protections against surveillance.").

4. *See* Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1624–25 (1999) (discussing how third parties may access cookies detailing another individual's browsing habits).

interfere with personal autonomy.[5] Surveys, high-profile litigation, and policy debates show the high levels of concern that people have about their information privacy in this context.[6]

The second change is a modification in the process of creating content. Technologies such as cloud computing and social networking—reinforced by the globalization of information flows—were decentralized. The Internet evolved from a linear model with a strong separation between content creators and content providers to a system characterized by global collaboration—sometimes called peer-to-peer technology or web 2.0.[7] A paradigmatic example of this trend was the appearance of Napster in the 1990s, which mass-marketed the idea that users could get files directly from each other (peer-to-peer).[8] The same mechanism was adopted by countless websites, such as YouTube, Wikipedia, and SSRN, and by the idea of blogs and social networks. This mechanism of content creation, as will be explained later,[9] is linked with the incentives to generate information.[10]

These changes made privacy law more prominent.[11] Perhaps the best example of this trend is the European Union (EU), where they motivated the EU data-protection framework—perhaps the most prominent omnibus approach to regulating privacy.[12] Many consider the EU data-protection

---

5. *Id.* at 1661 (discussing the "autonomy trap" associated with digital participation).

6. For a review of different surveys reaching this conclusion, see Jeff Sovern, *Opting in, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1053–55 (1999).

7. LAWRENCE LESSIG, CODE 2.0, at 34 (2006).

8. This phenomenon has motivated commentaries assessing its effects in copyright law, and evaluating modifications for it. *See, e.g.*, Daniel Benoliel, *Copyright Distributive Injustice*, 10 YALE J.L. & TECH. 45, 57–58 (2007); Raymond Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263, 272–73 (2002); Niels Schaumann, *Copyright Infringement and Peer-to-Peer Technology*, 28 WM. MITCHELL L. REV. 1001, 1040 (2002).

9. *See infra* Part II.

10. *See infra* Part II.

11. Alessandro Acquisti, Leslie John & George Loewenstein, *What is Privacy Worth?*, 42 J. LEGAL STUD. 249, 250 (2013).

12. The central norms of the framework are the Council Directive 95/46, art. 3, 1995 O.J. (L 281) 31, 39 (EC), Council Directive 2002/58, art. 3, 2002 O.J. (L 201) 37, 43 (EC), Council Directive 2009/136, art. 1, 2009 O.J. (L 337) 11, 21 (EC), and the Consolidated Version of the Treaty on the Functioning of the European Union art. 49, 56, 114, Oct. 26, 2012, 2012 O.J. (C 326) 49 [hereinafter

framework the leading paradigm in information privacy.[13] Several of the considerations that follow find their best examples in EU law.

Writings about privacy law often reflect the implicit idea that there is a tradeoff between privacy and the amount of information available to pursue other social goals, such as research that will in turn lead to innovation.[14] This tradeoff is sometimes depicted as a choice between rights and efficiency,[15] where we prioritize one or the other depending on our normative views. Sometimes, this tradeoff is implicit, when a balance between the right to privacy and the right to freedom of expression or to access to information is proposed. The idea that this tradeoff exists determines the extent to which normative arguments recommend protection of privacy. I argue here that such a tradeoff is inaccurate, and that realizing this can lead us to better information privacy law (IPL).

To illustrate this, one must evaluate the incentives generated by the creation of entitlements over personal information. In a low transaction-cost scenario where property

---

TFEU]. The EC has based its competence to issue these directives on the single market provision of TFEU article 114, referring also to articles 49 and 56 of the treaty (free movement of goods and services provisions). In *DocMorris* and *Gambelli*, the European Court of Justice (ECJ) has accepted the use of article 114 TFEU as a basis of competence for regulating the Internet. *See* JOHN DICKIE, PRODUCERS AND CONSUMERS IN EU E-COMMERCE LAW 23 (2005); *see also* Case C-322/01, Deutscher Apothekerverband v. DocMorris, 2003 E.C.R. I–14951; Case C-243/01, Gambelli, 2003 E.C.R. I–13033.

13. NEIL ROBINSON ET AL., REVIEW OF EU DATA PROTECTION DIRECTIVE, REPORT FOR THE UK INFORMATION COMMISSIONER'S OFFICE 22 (2009) (describing the Privacy Directive as a "reference model for good practice"); Paul Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1971 (2013) ("[T]he international debate about information privacy has never been confined to human rights or data trade. It has always been about both."). More than thirty countries have followed this model. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 23 (2012). This is largely driven by the prohibition of companies in the EU from sending data to companies in countries outside the union without guarantees that such data will receive an equivalent protection as it would have in the EU. *See* sources cited *supra* note 12.

14. *See, e.g.*, AMITAI ETZIONI, THE LIMITS OF PRIVACY 150 (2008) (discussing the privacy implications of computerized medical records); *see also* WORLD ECON. FORUM, PERSONAL DATA: THE EMERGENCE OF A NEW ASSET CLASS (2011).

15. *Cf., e.g.*, C. Dennis Southard IV, *Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store, and Distribute Information*, 9 COMPUTER L.J. 359 (1989). As a partial disagreement, one should note that rights are important for most conceptions of efficiency.

rights are clearly defined, the allocation of an entitlement should not affect Kaldor-Hicks social welfare,[16] since costless bargaining will lead to its *ex post* allocation to its highest valuer. However, there is a caveat to this principle for goods that are not yet available in the market.

From this viewpoint, we can differentiate two categories for the purposes of this article: undisclosed information about oneself that is therefore unavailable for others to use, which I will call personal data, and information about oneself that was disclosed and is therefore available, which I will call personal information.

I argue that the production caveat to the irrelevance of allocation includes personal data because they do not have the characteristics of a good until the data are disclosed and made available for others to use. In those cases, the entitlement is relevant to determine investment levels, and hence the quantity of information that will be available in the future. To disclose personal data and make it available to others (turning it into information), people face expected costs that, if left uncompensated, lead to worries and, in turn, a lower level of disclosure.

The public good characteristics of information provide an additional reason to be concerned with these investment levels.[17] If personal information has non-internalized positive spillovers, its underproduction effect will be exacerbated because the producer will not capture the full benefits of production. Hence, establishing data-protection rules is not simply defining entitlements over available goods over which there could be a dispute. Establishing data-protection rules is also defining entitlements over goods that are not yet available, where generating them implies expected costs for those who can produce them.

For these reasons, some degree of information privacy increases the amount of personal information available for exchanges. It is incorrect that privacy reduces the scope of the

---

16. *See generally* J.R. Hicks, *Foundations of Welfare Economics*, 49 ECON. J. 696 (1939); Nicholas Kaldor, *Welfare Propositions of Economics and Interpersonal Comparisons of Utility*, 49 ECON. J. 549 (1939).

17. *See generally* Roger A. McCain, *Information as Property and as a Public Good: Perspectives from the Economic Theory of Property Rights*, 58 LIBR. Q. 265 (1988) (examining the public goods characteristics of information in the library context).

rights against which it is sometimes balanced, such as access to information. What is more, it also increases them. The normative question about information privacy then turns from whether to grant privacy at all to protect access to information, to how much privacy to grant to optimize access to information. Either no protection at all or a maximum level of protection would lead to a low amount of information available.

To address this normative question, I frame the protection of information through privacy as a mechanism to allocate entitlements over personal information, by virtue of which the entitlement-holder has the right to decide who can access it and who cannot (hence excluding others from accessing the information).[18] The establishment of entitlements is analytically prior to deciding how to protect it—e.g. by property rules—because one must determine whether an entitlement is in place to evaluate which protection is most appropriate for it.[19] In this sense, property is narrower than entitlements. Based on this consideration, I evaluate whether property rules, liability rules, or inalienability rules are the best way to protect privacy entitlements. Building on the economic considerations made, an optimal protection mechanism will combine different types of rules, and provide differing levels of exclusion (and sometimes no exclusion at all) depending on the type of information involved.

The approach I introduce here, in this way, addresses two gaps in the privacy literature. The question of why privacy is relevant is answered by seeing that transaction costs are not low and, more importantly, the placement of its entitlement matters for production. The question of how to introduce property elements over personal information given differences in the reasons to protect personal information and to protect intellectual property is addressed by showing that both copyright and IPL foster the generation of information.

---

18. This is a broad definition of entitlement, similar to the definition used by Calabresi and Melamed, which only entails that the good (in this case personal information) is owned by someone, and that such person has rights over it. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1089 (1972) ("[E]ntitlements are protected by property, liability, or inalienability rules . . . .").

19. *Id.* at 1090.

The next Part will review the traditional economic perspective on privacy: that the optimal scope of privacy protection is often no privacy at all. Part II will point to the special characteristics of personal information in the context described in this introduction: personal information is a public good, has low transaction costs of communication, and is a good that is not yet available (and often has high costs of production). Part III will evaluate the production of personal information, which is disclosed as a by-product of an activity and whose protection increases its production levels. These characteristics eliminate the central economic objection to privacy and thereby justify the creation of privacy entitlements. Part IV will evaluate the different ways of protecting these entitlements under a Calabresi and Melamed framework, examining whether property rules or liability rules are most appropriate. It will conclude that a mixed protection system can best address privacy issues. Part V will provide normative recommendations to structure this mixed protection system: IPL has common grounds with copyright, and it could be structured similarly to it, but it must pay special attention to some technological characteristics that are relevant in light of the considerations made in Part II. Part VI will conclude.

I. THE ECONOMICS OF PRIVACY

A. CONCEALMENT AND ASYMMETRIC INFORMATION

A well-known article on privacy by information economist Jack Hirshleifer began by stating that

> a new territory has been discovered by economists, the intellectual continent we call 'privacy.' The pioneers are our peerless leaders Posner and Stigler whose golden findings have already dazzled the world. . . . Our pioneering economists, like explorers in other places and other times, found aborigines already inhabiting the territory—in this case intellectual primitives, Supreme Court justices and such. Quite properly, our explorers have brushed the natives aside.[20]

The curious thing about this quote is that, contrary to what a hopeful reader might think, Hirshleifer was not sarcastic. The first economic account of privacy, well described by Hirshleifer, applies the Coase theorem to state that free exchange of data will take it to the party that values it the most independently of

---

20. Jack Hirshleifer, *Privacy: Its Origin, Function, and Future*, 9 J. LEGAL STUD. 649, 649 (1980).

who originally owns it. For that reason, whether there is a right to privacy is irrelevant because, in any case, market forces drive information to its highest valuer.

Such account of privacy, in some way, is a more formal version of the famous "I have nothing to hide" argument, and it has become a widespread reason among legal economists to disregard privacy claims.[21] The term "privacy" is taken to mean concealment of information—in particular, concealment of information in an instrumental way.[22] Seeing privacy as concealment links it with the economics of information, where one person wants to screen for a characteristic and another would like to conceal it (for example, in the job market), thereby impeding efficient allocations.[23]

According to this argument, privacy concerns are instrumental: people assert privacy rights to hide data from someone else to obtain something. There are individuals with bad traits who want to hide them (privacy) and individuals with good traits who want to show them. In this account, information is only an intermediate good that has costs of protection and discovery.[24] Privacy would then create an information asymmetry for those traits disadvantaging the buyers in the market (for example, employers), thereby distributing wealth and creating inefficiencies.[25] In this way, privacy as concealment

---

21. *See, e.g.*, Richard A. Epstein, *The Legal Regulation of Genetic Discrimination: Old Responses to New Technology*, 74 B.U. L. REV 1, 12 (1994) (describing privacy as "the right to misrepresent one's self to the rest of the world").

22. Richard Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 405 (1981) ("[P]rivacy as concealment of information seems the most interesting from an economic standpoint."); *see* Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 411 (1978) (describing the right to privacy as concealment of information as an unattractive approach); Richard Posner, *An Economic Theory of Privacy*, 2 REGULATION 19, 21 (1978) (discussing how information a person seeks to conceal may have value to others); *see also* Richard Posner, *Privacy*, *in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 103, 103–07 (Peter Newman ed., 1998).

23. Posner develops here the idea that privacy is a tool of concealment for the devious, originally formulated by Arndt. *See* Heinz Arndt, *The Cult of Privacy*, 21 AUSTL. Q. 68, 69 (1949) ("Most codes, whether they are embodied in law or merely in moral rules and social taboos, serve to protect individuals and society and against anti-social acts. The cult of privacy seems to serve the opposite purpose.").

24. *See* Posner, *An Economic Theory of Privacy*, *supra* note 22.

25. *Id.* For a different argument, stating that information about others is necessarily incomplete, and a lack of privacy rule can lead to hasty judgments

of data would reduce the information with which the market allocates resources.[26]

This idea of privacy equates it to restricting knowledge. Privacy reduces the amount of information available about someone. People who want information protected by a privacy statute will accordingly use other less precise (and usually less intrusive but more costly) substitutes as a proxy for the data they want to acquire. For example, if an employer cannot access the work history of a potential employee, she will establish a trial period in which she will monitor the new employee.[27] A similar principle can be applied to the Internet: if the same employer cannot access criminal records, she will estimate the likelihood that the employee has a criminal record based on the information she has available.

The next step in the argument applies the Coase theorem. With clearly defined property rights and low transaction costs, goods will end up in the hands of those who value them the most, independent of their initial allocation.[28] Under these conditions, the party that values a good the most can buy it from the other if the initial allocation was granted to the latter.[29] It is sometimes argued along these lines that, if one applies this argument to personal information, as long as transaction costs

---

about others that are often mistaken, see Daniel Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1039 (2003) ("[I]solated information, often constituting only part of a very complicated reality, may lead to hasty condemnation."). For the argument that the Internet is prone to disseminating false rumors, see Cass Sunstein, *Believing False Rumors*, *in* THE OFFENSIVE INTERNET 91 (Saul Levmore & Martha Nussbaum eds., 2010).

26. Still, Posner argues that the privacy tort is efficient. The tort covers four aspects: preventing the use of one's picture and name without one's consent for advertising purposes, preventing facts about one being portrayed under a "false light," preventing people from obtaining information by intrusive means, and preventing the publication of intimate facts about oneself. Posner argues that the first three increase the flow of information and that the prevention of publication of intimate facts is rarely enforced. *See* Posner, *The Right of Privacy*, *supra* note 22.

27. *Cf.* George Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 632 (1980). In these contexts, not disclosing information can sometimes also be informative for the other party: if people with good traits can reveal them, but people without them cannot do so fraudulently, then the lack of disclosure will be informative of the lack of good traits.

28. Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 16 (1960).

29. *Id.*

remain low, whether there is privacy (which allocates the right over information to the person to whom that information refers) or no privacy (which allocates information to whoever finds it) is irrelevant for the information's final allocation.[30] Privacy law would then have no welfare effect. For that reason, under this no-transaction-cost condition, introducing disturbances in the market such as welfare-decreasing information asymmetries that generate the need for proxies would be unjustified.[31]

B. PRIVACY'S LACK OF ECONOMIC RATIONALE

The traditional literature on the economics of privacy seems to indicate that there is little economic justification for a general right to privacy. This reluctance to protect privacy, however, has been the subject of two attacks: one arguing that it is based on (and depends on) the overly narrow conception of privacy as concealment,[32] and one arguing that it ignores relevant externalities in data trading.[33]

Regarding the conceptual critique, the concealment approach, which considers privacy socially welfare-decreasing, does not take into account that privacy can also have a non-instrumental value.[34] Surveys have shown that people do not believe that those concerned about their privacy try to hide immoral or illegal behaviors,[35] and this result is confirmed by psychological literature on the topic.[36] People have "pure" privacy preferences that are independent of considerations of reputation or deceit—they consider privacy valuable in itself.[37]

---

30. *See generally* Posner, *The Economics of Privacy*, *supra* note 22; Posner, *An Economic Theory of Privacy*, *supra* note 22; Stigler, *supra* note 27, at 981.

31. *See* Posner, *The Economics of Privacy, supra* note 22; Posner, *An Economic Theory of Privacy*, *supra* note 22; Stigler, *supra* note 27, at 981.

32. Edward Bloustein, *Privacy is Dear at Any Price: A Response to Professor Posner's Economic Theory*, 12 GA. L. REV. 429, 439 (1978).

33. *See* Kenneth Laudon, *Markets and Privacy*, 39 COMM. ASS'N COMPUTING MACHINERY 92, 92–94 (1996).

34. *Id.*

35. PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 48 (1995).

36. *E.g.*, Cathy Goodwin, *A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption*, 1 J. CONSUMER PSYCHOL. 261 (1992).

37. M. Ryan Calo, *The Boundaries of Privacy Harm,* 86 IND. L.J. 1131, 1142–43 (2011) (defining subjective privacy harms as those that "flow from the perception of unwanted observation"); *see also* Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061 (2009) (discussing the social costs

These are likely motivated by reasons such as improving the consumption experience and eliminating interference by disapproving peers.[38]

A situation in which individuals own their personal information can be seen as welfare-enhancing because of pure privacy preferences that form part of Internet users' utility functions.[39] This preference encompasses a taste for privacy in contexts where the individual wants to keep data private for reasons other than deception.[40] Given these preferences, there is no reason to assume that, in interactions not mediated by consent, the gain for the acquirers of an Internet user's information is always larger than that person's loss. If *A* acquires *B*'s personal information without her consent, we often cannot know if *A*'s utility is larger than *B*'s disutility. If the law established a right over personal information, however, those preferences would be reflected in a consensual agreement.[41]

The second critique of the traditional literature is that it ignores the externalities in information processing.[42] A privacy interest is implicated every time information about someone is collected or used without her consent, potentially imposing an externality on her. The private cost of collecting personal information in this circumstance is lower than the social cost. Therefore, more personal information is collected than socially

---

and benefits associated with privacy related legislation, including legal frameworks for the disclosure of personal information).

38. *See* Goodwin, *supra* note 36, at 263.

39. Posner also recognizes the relevance of pure privacy preferences in later work regarding governmental surveillance. Richard Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 245–46 (2008).

40. *See* Laudon, *supra* note 33, at 93 ("Privacy is a moral claim of individuals to be left alone and to control the flow of information.").

41. *See* Richard Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2382 (1995); James Rule & Lawrence Hunter, *Towards Property Rights in Personal Data*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 168 (Colin Bennett & Rebecca Grant eds., 1999).

42. *Cf.* Corien Prins, *When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?*, 3 SCRIPT-ED 270, 277 (2006) ("[P]rivacy can be understood as a problem of social cost, where the actions of one agent (e.g., a mailing list broker) impart a negative externality on another agent (e.g., an end consumer).") (internal quotations omitted).

efficient.[43] As long as the collector and not the Internet user owns the personal information, people are not compensated for the use of their personal information, and the price of such information is too low because it fails to reflect the cost that its use implies for them.[44] Secondary use of information also poses externalities to Internet users, which come in the form of annoyances, such as spam, that consume time and attention.[45] Giving users control over the transfer of their information (making their agreement needed for further trade) would internalize these externalities.[46]

The use of encryption has been suggested as a way to approximate protection "from below" in the absence of legislation that establishes it.[47] Encryption allows an individual to exclude others from information, and hence should allow for bargaining and redistribute wealth to consumers.[48] The inconvenience of this approach is that it can be costly for Internet users to engage in encryption and, even if they do, the aggregated cost of self-protection would be socially wasteful.

The critiques raise more questions than they provide answers. The first critique (conceptual) does not show that more ample concepts of privacy would lead to alternative economic justifications that trump the early arguments on the economics of privacy. The second critique (concerning externalities) leaves a central issue unanswered: if transaction costs are low, then as long as the property rights are clearly defined, the entitlement's

---

43. *See* Laudon, *supra* note 33, at 99 (describing the phenomenon of a National Information Market, where market mechanisms equilibrate supply and demand of information).

44. *See* Kenneth Laudon, *Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (Barbara Wellbery ed., 1997), https://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age.

45. If someone gives her telephone number to a company so it can fix her cable, and then the company gives it to someone else that calls her at dinnertime to sell her an insurance policy, that is a cost (in the form of attention and time that is taken from her) that is externally imposed from the transaction between the cable company and the insurance company. *See* Hal Varian, *Economic Aspects of Personal Privacy*, *in* CYBER POLICY AND ECONOMICS IN AN INTERNET AGE 127 (William Lehr & Lorenzo Pupillo eds., 2002).

46. *Id.*

47. Eli Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, *supra* note 44, at 21.

48. *Id.*

allocation should be irrelevant for total welfare, as the allocation will not change who will hold the right *ex post*. In addition, the reason why each agent values the good at any amount, and whether there are any externalities, should also be irrelevant, because low transaction costs allow for a bargaining process that would internalize them, unless distribution matters.[49] The following Parts explain how efficiency considerations can justify IPL.

II. CHARACTERISTICS OF PERSONAL INFORMATION ONLINE

A. PUBLIC GOOD

A central characteristic of information is that people can make use of it without leaving less for others and, for digitalized information, it is easy to reproduce.[50] Information, for this reason, has public good characteristics: once released, it can be reproduced at a marginal cost close to zero making it difficult to monitor and control who has it (non-excludability), and the use of information does not reduce the amount left available to others (non-rivalry).[51]

Even before Samuelson's seminal work on public goods,[52] works of authorship were described as having the features of non-excludability and non-rivalry due to the characteristics of information.[53] Shortly after, information was identified as a public good that suffers from the problems of both non-excludability and non-rivalry.[54]

---

49. *See* Coase, *supra* note 28.

50. *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1196 n.8 (1998) ("The digitalization of information makes simple the reproduction and quick transmission of perfect copies through cyberspace.").

51. Stigler, *supra* note 27; *see* Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2004) (discussing, at points, the market failure associated with non-rivalry).

52. Paul Samuelson, *The Pure Theory of Public Expenditure*, 36 REV. ECON. & STAT. 387 (1954).

53. *See, e.g.*, ARNOLD PLANT, THE NEW COMMERCE IN IDEAS AND INTELLECTUAL PROPERTY (1953); Arnold Plant, *The Economic Aspects of Copyright in Books*, 1 ECONOMICA 167 (1934).

54. *See, e.g.*, Stephen Breyer, *The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs*, 84 HARV. L. REV. 281 (1970) (advocating for copyright as a solution to these public good problems);

Due to its public good characteristics, the generation of information produces positive spillovers to people other than its creators.[55] These positive spillovers, or positive externalities, imply that the creator does not internalize all social benefits from generating information and, for that reason she has suboptimal incentives to produce it.[56] For this reason, it might be socially welfare-increasing in the long run to allow for greater internalization and thereby incentivize information production in order to ensure that a socially desirable amount is produced.[57]

Personal information—a type of information—features these characteristics. Given that information has a cumulative nature (its uses are not independent but build on each other),[58] it behaves as a capital good that will present most of its benefits in the future. Therefore, it is difficult to grasp the effects of different kinds of information, or even information in general, unless we take into account its long-term consequences.[59] Inasmuch as information presents the characteristics of a public good, it would be socially desirable to incentivize the generation of more information, as well as its dissemination, which we can call information flow.[60] The next sections explore how privacy relates to this aim.

B. LOW COMMUNICATION COSTS

Technological changes reduced the transaction costs of gathering, storing and disseminating information; in addition,

---

Robert Hurt & Robert Shuchman, *The Economic Rationale of Copyright*, 56 AM. ECON. REV. 421 (1966).

55. *See, e.g.*, Stigler, *supra* note 27.

56. *See generally id.*

57. *See* Wendy Gordon, *Asymmetric Market Failure and Prisoner's Dilemma in Intellectual Property*, 17 U. DAYTON L. REV. 853 (1992) (analyzing along these lines in the form of a prisoners' dilemma where agents choose whether to produce or reproduce information in the context of intellectual property).

58. *See generally* William Landes & Richard Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 325–27 (1989).

59. From this perspective, information is socially valuable in a way that is difficult to quantify. Determining how far in the future one wants to look and what discount rate one wants to apply are only the first obstacles to specification of its social benefits. This is also the case, for example, of environmental goods. *See, e.g.*, Heinz Kurz, *Goods and Bads: Sundry Observations on Joint Production, Waste Disposal, and Renewable and Exhaustible Resources*, 3 PROGRESS INDUS. ECOLOGY 280 (2006).

60. *See, e.g.*, Murphy, *supra* note 41.

Internet users voluntarily give personal information via peer-to-peer sharing.[61] These characteristics make the marginal cost of acquiring information close to zero.[62] In the context of information technology, personal information exchanges have strikingly low costs of communication.[63]

In the old days, when someone wanted information about someone else, she would incur costs to obtain the data. These costs were incurred, for example, in chasing a celebrity in the street to take pictures of her, eavesdropping on a conversation behind a door, peeking through a keyhole, or wiretapping a telephone line. Some current ways of acquiring information about someone, such as compromising their cybersecurity with a virus or looking for their information in search engines, follow a structure similar to the traditional market for personal information. However, they present lower transaction costs—a script can do the work that in other times required personnel and expensive equipment.[64] Using these tools, the person who desires information must engage in some degree of search costs to acquire it, but these costs are often lower than those of traditional privacy invasions.[65] Looking for someone's details in a search engine, for example, is easier and less costly than going through her correspondence, wiretapping her telephone, or questioning her friends.

The market for personal information online, oftentimes, does not follow this pattern due to its different technological characteristics: reduced costs and peer-to-peer sharing.[66] In some markets for personal information online, where online profiling is used,[67] the information producer (Internet user) puts

---

61. *See, e.g.*, Schaumann, *supra* note 8, at 1002.

62. *See* Ku, *supra* note 8, at 274.

63. *See, e.g.*, Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1 U. CHI. LEGAL F. 217, 231 (1996) (commenting that, for low transaction-cost situations, a "property entitlement for such items seems sensible").

64. *See* Schwartz, *supra* note 4, at 1619 (attributing the Internet's prominence in information "production, distribution, and manipulation . . . [to its] impressive ability to increase the speed and lower the costs of transferring and sharing information").

65. *Cf. id.*

66. *Cf.* Sovern, *supra* note 6 (discussing how to further reduce consumers' transaction costs for privacy protection).

67. Profiling is the assembling of personal information from different sources to generate a complete database of an Internet user. *See, e.g.*, Roger Clarke, *Profiling: A Hidden Challenge to the Regulation of Data Surveillance*, 4 J.L. & INF. SCI. 403, 404–05 (1993).

the information in the acquirer's hands, seemingly for free.[68] Under this mechanism (described before as the peer-to-peer or Web 2.0)[69] the acquisition of information has not merely a reduced marginal cost compared to the traditional privacy scenario, but a marginal cost of zero.

This mechanism can operate through monitoring active and passive digital footprints.[70] Regarding active digital footprints, social network companies do not need to incur additional costs to discover personal information about their users because, by utilizing the social network, the users provide that information by themselves.[71] Similarly, the other users do not need to ask their friends and acquaintances for their recent pictures and updates because they often send them through the social networks. Cloud computing companies, similarly, do not need to inquire about which kind of files their users manage because, by using the cloud computing service, the users show that information to the companies voluntarily.

Regarding passive digital footprints, the Internet has technologies such as http cookies and fingerprinting that create data trails without the user attempting to do so—and the technologies can do this without the user's knowledge.[72] Even technologies not specifically designed to create data trails generate user-metadata associated with the places where the user places attention, and therefore also collect information.[73]

---

68. Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015) (weighing the possible benefit and detriments of the fact that we now share information online, "both knowingly and unwittingly – to one another, to commercial entities, and to our governments").

69. LESSIG, *supra* note 7.

70. *See, e.g.*, *Digital Footprint*, TECHTERMS, https://techterms.com /definition/digital_footprint (last visited Feb. 5, 2017) ("A 'passive digital footprint' is a data trail you unintentionally leave online [like your browsing history]. . . . An 'active digital footprint' includes data that you intentionally submit online [like sending an email].").

71. *E.g.*, *id.* ("[P]osting social media updates are another popular way to expand your digital footprint."). These companies have built an infrastructure that represents fixed costs, while the marginal costs of acquiring information from Internet users is close to zero.

72. *See* Schwartz, *supra* note 4, at 1624–25.

73. *Id.* at 1625 ("Once Web sites identify a specific visitor, they can match her to their rich stores of 'clickstream data,' which is information about the precise path a user takes while browsing at a Web site, including how long she spent at any part of a site.").

The counterpart to this reduction in the cost of collecting and disseminating information is the increased cost of protecting one's personal information. Surveillance is more difficult to detect in cyberspace than in physical spaces, which means that preventing such surveillance is more costly.[74]

Protecting one's privacy on the Internet requires technical skills that not all Internet users possess and, for those who do, this protection is costly.[75] The tradeoff between the benefits obtained for data disclosures and their expected privacy cost is opposed to another tradeoff between privacy and convenience. For example, browsing through anonymity networks such as TOR—one of the most effective means of self-protection—leads to a reduction in usability (for example, users need to retype all registration data on each access) and to a decrease in browsing speed.[76] Moreover, monitoring one's personal information after disclosure is rarely possible and, when so, is costly.[77] There is as of yet no equivalent for the Internet to the sealed envelopes for postal secrecy, which could easily tell us if someone opened our correspondence and tip us off on what they could have learned.[78]

C. A GOOD THAT IS NOT YET AVAILABLE

Irrespective of low transaction costs and clearly defined rights, entitlements' allocations have distributional effects.[79] If *A* values a good more than *B*, and the entitlement over it is given to *A*, *B* can obtain the good only after bargaining with *A* if protected by property, or compensating *A* if protected by liability. Although irrelevant for total welfare, both *A* and *B* care about who initially has the entitlement. *B* had to give something to *A* to obtain the good; if *B* had been given the entitlement in

---

74. *See* Clarke, *supra* note 67 (presenting an early argument for regulation in this area).

75. Moreover, this could be considered suspicious behavior, and result in increased governmental surveillance.

76. *See Tor: Overview*, TOR, https://www.torproject.org/about/overview (last visited Feb. 5, 2017) (providing "both organizations and individuals [the ability] to share information over public networks without compromising their privacy").

77. *See id*. TOR provides an anonymized pathway to prevent surveillance of Internet traffic. *Id.*

78. *See* Susan Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1 (2005).

79. *See generally* Coase, *supra* note 28.

the first place, she would have been wealthier by the end of the transaction.

This distributional effect is relevant for the production of goods. If Internet user *A* is in a position to produce a good and trade with service provider *B* and, in contrast to the scenario in the last paragraph, the entitlement over that good is given to *B ex ante*, *A* will lack incentives to produce it.[80] Entitlements determine the incentives for investment to generate goods because they determine who will get paid in the trades that will take place if those goods exist.[81] Hence, it affects goods' production levels.[82]

The mechanisms to generate information either actively or passively described in the last section illustrate that the amount of personal information available is not fixed. A significant portion of such information is produced by users of these services depending on how much (and how many) services they consume. These data, in turn, do not fulfill the characteristics of a good until disclosed to others (becoming available information) because, before the disclosure takes place, they are not available for use and therefore unable to satisfy other people's needs.[83]

In turn, personal data disclosure by Internet users implies expected privacy costs—which depend on the type and amount of data disclosed. The more personal data disclosed by an Internet user in the use of these products, the higher the risk that she faces harm in the form of a privacy breach. This often leads Internet users, in the absence of regulatory protection, to engage in socially costly self-protection. Internet users face expected costs of privacy breach both in their initial production of information and the subsequent information trades between

---

80. This is analogous to the reason why most legal systems establish protections in the form of entitlements for intellectual property (i.e., to incentivize production in the first place), as it is evaluated below.

81. *See* Oliver Hart & John Moore, *Property Rights and the Nature of the Firm*, 98 J. POL. ECON. 1119, 1120 (1990); Thomas Merrill & Henry Smith, *Making Coasean Property More Coasean*, 54 J.L. & ECON. S77, S90 (2011); *see also* Thomas Merrill & Henry Smith, *What Happened to Property in Law and Economics*, 111 YALE L.J. 357 (2001).

82. *See* sources cited *supra* note 81.

83. Goods have been defined as materials that can readily satisfy human wants, and in such way, increase utility. *See* Murray Milgate, *Goods and Commodities*, *in* THE NEW PALGRAVE DICTIONARY OF ECONOMICS (Lawrence Blume & Steven Durlauf eds., 2008).

data collectors, intermediaries, and advertisers.[84] Information processing produces an externality problem[85]: the company that carries it out obtains the full benefits of processing—via marketing gains or fee gains with the sale of such information—but does not suffer the expected losses produced by such disclosure of personal data. Hence, it has incentives to overuse users' personal information.[86]

III. PRODUCTION OF PERSONAL INFORMATION ONLINE

A. BY-PRODUCT

Unlike standard goods, people do not produce their personal information deliberately to sell it to companies online.[87] App developers, for example, do not ask people directly at each moment where they are, but instead offer them a product to monitor their walking distances and calorie expenditure, which also records their location data.[88]

When Internet users consume goods such as an app or website, the website, or advertisers, can profit from their time and attention.[89] With goods like social networks and cloud computing, the good's consumption (time at the website) produces another good (personal information).[90] The more someone uses Facebook, the more Facebook knows about her, and the more files she uploads to Dropbox, the more Dropbox

---

84. *See* John Hagel & Jeffrey Rayport, *The Coming Battle for Consumer Information*, 75 HARV. BUS. REV. 53 (1997).

85. *See, e.g.*, Laudon, *supra* note 33; Varian, *supra* note 45.

86. PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998).

87. This has some exceptions, such as autobiographies. *Cf.* Murphy, *supra* note 41, at 2408–10 (recounting a breach of privacy, when a psychiatrist's biography improperly reported details of a confidential counseling session).

88. *See generally* Richard Cornes & Todd Sandler, *Easy Riders, Joint Production and Public Goods*, 94 ECON. J. 580 (1984).

89. *See* Alexander Furnas, *It's Not All About You: What Privacy Advocates Don't Get About Data Tracking on the Web*, ATLANTIC (Mar. 15, 2012), https://www.theatlantic.com/technology/archive/2012/03/its-not-all-about-you-what-privacy-advocates-dont-get-about-data-tracking-on-the-web/254533/ ("The Internet of free platforms, free services, and free content is wholly subsidized by targeted advertising, the efficacy (and thus profitability) of which relies on collecting and mining user data.").

90. *See, e.g.*, Clarke, *supra* note 67, at 409 (discussing the potential downsides of acquisition of personal information from profiling).

knows about her. This personal information is useful to the service providers because it allows them to not only show advertisements but also personalize their content, increasing ad relevance and thus the sales of the products advertised.[91]

From this perspective, personal information is a by-product of the activity of using the product. For the user, consuming a social network is tied to producing personal information. This exchange functions differently than those of standard goods. When users generate personal information by using the product, they do not produce a good deliberately. People do not say, for example, "I need to generate more personal information to buy more time at Facebook"; they just know that the more they use the product, the more personal information about them that will be in the market. While they consume the web service, they produce personal information, which is a good for the service provider.

Generating this product has an expected (private) cost: the increased risk of a privacy leak together with the disutility of sharing personal information from pure privacy preferences.[92] The dissemination of personal information (information processing), as it increases the probability of a privacy leak, creates in rational users an expected cost function for the production of personal information which, when it gets too high, stops them from continuing to use the product.[93] They weigh the marginal benefit of using the website against the marginal cost of disclosure.[94]

A data-protection statute does not have the same effect in this context as the effect for traditional privacy exchanges described by the first-generation economics of privacy.[95] The by-product characteristic of personal information accounts for why it is produced even in the absence of exclusion rights, and at the same time why there are limits on its production.

Picture someone using a web service, where her consumption is measured by the extent of the service's use. As she uses the web service, she produces as a by-product the

---

91. *See id.* (warning that such advertising can "cross[ ] a boundary to become consumer manipulation").

92. *See* Kang, *supra* note 50, at 1246 (discussing motivating factors for the consumer to withhold private information).

93. *See id.*

94. *See, e.g.*, *id.* at 1247.

95. *See supra* Section I.B (discussing first-generation economics of privacy).

personal information shared. The web service cannot be consumed separately from producing information: if she spends time in the network, personal information about her will be available to the service providers. The production of information, in turn, has the cost for the user of expected privacy breach and disutility from sharing, where the more information shared, the higher the risk of a privacy breach.[96] The Internet user's utility from using the web service is determined by how much she uses it.[97] Her expected utility function is formed by the utility from using the web service minus the cost of producing the information.[98]

Maximizing the Internet user's utility function results in limiting her web service's consumption to the point where her marginal benefit of consuming the website equals her marginal cost of producing information.[99] After this point, the cost of producing information is too high for her. Because the website cannot be consumed without producing information, the Internet user stops consuming it. Thus, the web service's level of use is limited by the production costs of personal information.[100]

This mechanism is seen, for example, with people who do not have a social network account because of privacy concerns although they otherwise would like to have one. The social network could profit from them, and they could profit from using the social network if there were a way for them to use the product without revealing personal information and receiving only non-personalized advertisements.

This scenario is the result of an asymmetric information problem that prevents these users from accessing the product because the service provider ignores the exact privacy sensitivity of its consumers.[101] This problem prevents the service provider

---

96. *Cf.* Noam, *supra* note 47 (discussing the Internet consumer's privacy-based motivations).

97. *Cf. id.*

98. *Cf. id.*

99. A special case would be one in which the marginal cost curve always lies above the marginal utility curve, and hence the two curves do not intersect. This would be the case of people with high pure privacy preferences, who do not share personal information.

100. This is often the case in environmental economics, with the difference that, in such cases, the by-product is often a bad instead of a good. *See* Kurz, *supra* note 59, at 282.

101. For a discussion on the asymmetric information problem of privacy, see generally sources cited, *supra* note 22.

from perfectly distinguishing among its users based on how privacy sensitive they are: the provider cannot distinguish between consumers based on the shape of the consumers' cost functions and allow some of them to consume the product while producing a smaller amount of personal information.[102]

However, social networks are able to partially discriminate among Internet users according to their sensitivity by offering different menus to choose from, which can function as a signaling device. These devices are different combinations of privacy settings and website functionality.[103] This choice allows Internet users to have different degrees of privacy preferences in the product, choosing the available combination that best satisfies their preferences.[104] Hence, Internet users can choose the combination that gives them the highest utility, allowing for the possibility of a separating equilibrium based on their privacy sensitivity.[105]

A very high level of privacy that takes a regulatory approach to protecting data and limits information's alienability would disallow Internet users to produce certain levels of information and, in such a way, would restrict the scope of possible choices. This would not only restrict the web service's business model but also reduce Internet users' utility. In this scenario, it would be better for IPL to adopt an approach closer to contract law and focus on enforcing the voluntary choices of the users and the network, and ensuring that they are made with informed consent. A privacy approach that allowed Internet users to trade, and thus gave them freedom of choice to express their privacy preferences, would accomplish this task.

B. EFFECT OF PRIVACY ON INFORMATION PRODUCTION

Under a static or allocative analysis, information is inversely related to the degree of privacy: the less privacy protection, the fewer rights that people will be able to exert over

---

102. *See generally* sources cited, *supra* note 22.

103. *See generally id.*

104. *Cf. id.* For example, Google and Microsoft do this for their email services, and Facebook does so for its social network.

105. If personal information were not a by-product, services such as social networks would only have incentives to offer this kind of product differentiation due to the pressure of competition. *See* Ruben Rodrigues, *Privacy on Social Networks*, *in* THE OFFENSIVE INTERNET, *supra* note 25, at 237 (addressing the effect of competitive pressure on product differentiation for social networks).

pieces of information, and the more personal information that will be available. This was the underlying idea in the first-generation literature on the economics of privacy.[106]

Under an analysis that includes dynamic effects, however, because personal data has the characteristics of a good that is costly to produce and is not yet available, the disclosure of personal data largely depends on the entitlement's allocation.[107] Allocating the entitlement to Internet users through privacy, therefore, becomes relevant. Some degree of privacy incentivizes the generation of information and, consequently, an increase in information flow, because privacy enables exchanges of pieces of information that would otherwise not be generated. This mechanism is similar to the exclusion from products protected under copyright law, which is weighed in the long run against access to creations that take place due to the incentives set by these laws.[108]

Consider as an example the number of people who, under current regulation, abstain from using social networks because of privacy concerns. With a higher level of privacy protection, these concerns would not arise or not be as significant, and those users would not need to abstain from using social networks. They would produce, in their use, information that under current regulation is not being generated.

This effect will be shaped by the entitlement's protection. A regime with no privacy at all would have a low level of information production (dynamic effect) but a high level of information flow of the information produced (static effect). A regime on the other end of the spectrum would produce the opposite result: a high level of information production (dynamic effect) but a low level of information flow (static effect). Due to the dynamic effect, a very low level of privacy would lead to a low level of information production because Internet users would

---

106. *Cf.* Murphy, *supra* note 41, at 2382 (stating that "the common law . . . from the get-go . . . has been hostile to privacy claims").

107. *See generally* Merrill & Smith, *What Happened to Property in Law and Economics*, *supra* note 81, at 375 (explaining the basis of entitlement).

108. While the static and dynamic effects work in opposite directions, it is likely that, up to a certain level of protection, the second overcomes the first in the long term. *See generally* Stanley M. Besen & Leo J. Raskind, *An Introduction to the Law and Economics of Intellectual Property*, 5 J. ECON. PERSP. 3, 11–18 (1991) (explaining this logic in Intellectual Property). A closer evaluation of the common elements between IPL and copyright is done below in Part V.

be under-incentivized to produce such information. Due to the static effect, an extremely high level of privacy protection would lead to little information flow because little would be shared.[109]

Due to this interrelation between the static effect on information flow and the dynamic effect on the generation of information, the relationship between privacy and the amount of personal information seems to follow a hill-shaped concave function. To maximize the amount of information in the market, the law must set a level of privacy high enough to incentivize information production, but not so high as to halt information flow. This relationship is illustrated in Figure 1.

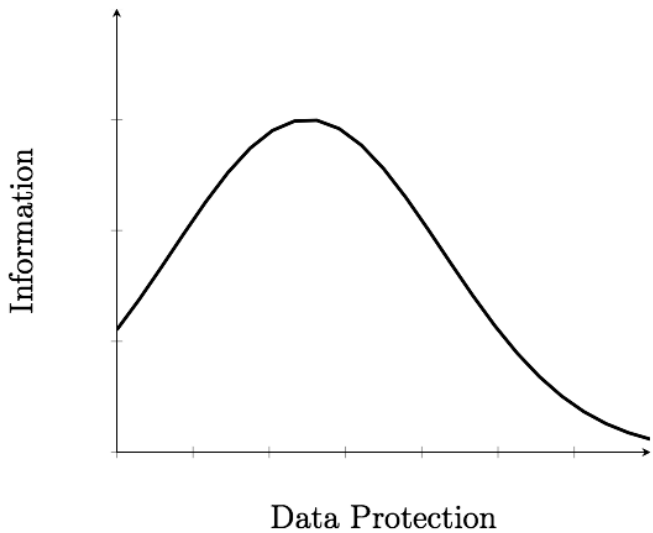

Figure 1. Illustrating the Relationship Between Data Protection and Amount of Information

A caveat to this argument is that some amount of personal information is likely to be produced even in the absence of IPL. In the function mentioned, the curve would therefore intersect the *y*-axis above zero. The explanation is that, as the previous

109. This would be a more extreme system than that of PETs, see *supra* Section III.A, which seek to allow for high privacy preservation while allowing the sharing of high-value data for socially valuable aims such as research. A PET-based system, in the ideal types identified here, also lies in the middle of both extreme regimes.

section showed, personal information is produced as a by-product of online activity.

In sum, due to the technological characteristics that underpin personal information online, the costs of communicating information are low, but this says little about the costs of transacting over the entitlement. Moreover, the current arguments fail to consider how the level of privacy increases the supply of information. For this reason, the objections to privacy protection often invoked in the economics literature are largely inapplicable to contemporary IPL.

Having established that the entitlements over personal information allocated by IPL are desirable, we turn to ask how to best protect them.

IV. PROTECTION MECHANISMS

A. PROTECTING PRIVACY WITH PROPERTY

From an efficiency point of view, one can distinguish three types of protection over entitlements: property, liability, and inalienability rules.[110] We can ask, under this framework, which of these three is an efficient mechanism to protect privacy entitlements.

Entitlements protected by a property rule can only be transferred with the title-holder's consent and in exchange for a price determined through bargaining.[111] Those protected by a liability rule, on the other hand, can be transferred without the title-holder's consent and in exchange for a collectively determined price.[112] Liability rules are used mainly due to high transaction costs of *ex ante* bargaining—or an actual impossibility.[113] Entitlements protected by an inalienability rule are not transferable, and if the transfer somehow takes place, the law sets back or nullifies the transfer to the extent possible.[114]

---

110. *See* Calabresi & Melamed, *supra* note 18.

111. *See id.* at 1106 (stressing the need to enforce voluntary contracts during transfers).

112. *See, e.g.*, *id.* at 1107–10 (identifying eminent domain as one of several examples of liability rules in use).

113. *See id.* at 1110 (stating that "efficiency is not the sole ground for employing liability rules rather than property rules").

114. *Id.* at 1092–93 ("An entitlement is inalienable to the extent that its transfer is not permitted between a willing buyer and a willing seller.").

Property rules have been proposed as a protection mechanism that could forbid extracting information from Internet users without their consent, hence protecting their privacy.[115] Property-rule protection of personal information can be portrayed as a non-collection default, which applies unless consent is given.[116] If the individual to whom the information refers has an entitlement over it, and it is protected by a property rule, she can control the dissemination of her personal information after it is disclosed.[117] On the other hand, if data collectors own the entitlement, then the default is collection.[118]

The non-collection default rule (a privacy rule) has been considered welfare increasing for three reasons.[119] The first reason is that technologies have decreased the transaction costs of acquiring people's personal information—once it is produced.[120] But these costs are asymmetric: if entitlements with a property rule were given to data collectors, individuals would face high costs for knowing what information about them was disseminated or will be disseminated—which is needed to engage in negotiations. This cost would be low for data collectors.[121] This implies that overall transaction costs would be

---

115. *See, e.g.*, Murphy, *supra* note 41; Prins, *supra* note 42, at 271 ("With the growing economic importance of services based on the processing of personal data, it is clear that ownership rights in personal data become the key instrument in realizing returns on the investment."); Schwartz, *supra* note 51.

116. *See* Calabresi & Melamed, *supra* note 18, at 1092 (explaining that "entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller"); Ignacio Cofone, *The Way the Cookie Crumbles: Online Tracking Meets Behavioural Economics*, 25 INT'L J.L. & INFO. TECH. 38 (2016) (explaining the dynamic of non-collection default rules).

117. *See* Calabresi & Melamed, *supra* note 18 (stating that each party gets to determine how much the entitlement is worth to them).

118. Murphy, *supra* note 41.

119. These have been formulated with the language of property rights. Under the Calabresi and Melamed framework, a property right is a type of entitlement that can be protected by a property rule, a liability rule, or an inalienability rule. However, when someone refers to a property right, they often mean one protected by a property rule. One can see from the language used in the literature, and also by the emphasis placed on consent, that the arguments are made with a property rule in mind. *See, e.g.*, *id.*

120. *See* Kang, *supra* note 50.

121. *See id.* (explaining that the harvesting of data is done automatically by computers at little cost).

reduced if the entitlements over personal information were allocated to Internet users with a property rule.

Under a regime with no privacy, companies lack incentives to make it easy for Internet users to control their personal data.[122] Giving rights over such information to users would force a negotiation that would alter this.[123] Privacy-enhancing technologies (PETs) are a response from users to this lack of protection, allowing them a higher level of control over their personal information.[124] Some consider these market-based mechanisms desirable in the face of new technologies.[125] However, self-protection implies costs that would be spared with a property rule.[126]

Property rules would allow for a market for personal information in which each Internet user could negotiate with firms regarding which uses they are willing to allow with regards to their personal information and for what compensation.[127] By becoming owners of their personal information, Internet users would be able to extract more for its release than under a no-property rule, and they would receive

---

122. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); *see* LESSIG, CODE 2.0, *supra* note 7, at 218 (explaining how the absence of incentives to maintain privacy interferes with our "desire to live in separate communities, or among or within separate normative spaces," and how this could have dangerous consequences for, as an example, "a gay man in an intolerant small town").

123. *See* LESSIG, CODE 2.0, *supra* note 7; *see also* Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

124. *See* GW VAN BLARKOM ET AL., HANDBOOK OF PRIVACY AND PRIVACY-ENHANCING TECHNOLOGIES, THE CASE OF INTELLIGENT SOFTWARE AGENTS 33 (2003) (stating that typical PETs include encryption tools and IP masks).

125. *See* Laudon, *supra* note 33 (advocating one solution to the problem).

126. *Cf.* Prins, *supra* note 42, at 277 (commenting that "although some try to protect their privacy by applying techniques to 'hide' their data, actual and effective transparency and control seems unattainable").

127. *See id.*; LESSIG, *supra* note 7, at 85–90, 229 ("[A] property rule . . . would reinforce whatever diversity people had about views about their privacy—permitting some to choose to waive their rights and others to hold firm."); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRACT. 56, 63–65 (1999) (arguing for a market solution to privacy problems); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 57–64 (1996) (discussing generally some theories of tort recovery for breaches of the privacy obligation); Murphy, *supra* note 41.

compensation for the expected privacy cost associated with each information disclosure.[128]

From the perspective of information production, we can add two reasons for the desirability of property rules. First, property rules would internalize *ex ante* the externalities of information processing (which increase the risk of privacy breaches) and would thereby incentivize information production.[129] Second, they would allow for subsequent sales once information is acquired—as with any product where when one can re-sell an item after buying it.[130] In this way, property rules would keep transaction costs low.[131] If companies had to ask Internet users for permission each time such information was traded, transaction costs would be too high, which would decrease information flow.[132] The ability to protect privacy without interfering with subsequent sales is, from this perspective, a desirable attribute of property rules.

B. DRAWBACKS OF PROPERTY RULES IN IPL

Despite their advantages, property rules could generate new problems in the interaction between Internet users and data collectors and processors. Namely, ineffectiveness due to bargaining positions, under-protection of information obtained through data mining, and a principal-agent problem.

Regarding bargaining, due to the type of interactions in which privacy policies are involved, where Internet users have a take-it-or-leave-it option, it is unclear to what extent property rules would improve their situation when compared to a no-

---

128. *See* Prins, *supra* note 42, at 271 ("[M]arket-oriented mechanisms based on individual ownership of personal data could enhance personal data protection. If 'personal data markets' were allowed to function more effectively, there would be less privacy invasion."); *cf.* Mell, *supra* note 127, at 26–27 (explaining that as it is now, individuals have little control over the exploitation of their personal information).

129. *See supra* Section II.E; *see also* Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* PRIVACY AND SELF REGULATION IN THE INFORMATION AGE, *supra* note 44, ch. 1, art. A ("The case for . . . self-regulation is especially strong, however, where there are important network externalities.").

130. *See* Eli M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, *in* PRIVACY AND SELF REGULATION IN THE INFORMATION AGE, *supra* note 44, ch. 1, art. B (arguing that if such sales are made illegal, it would not stop the sales from occurring, but merely cause sales to be more expensive).

131. *See id.*

132. *See id.* (stressing the importance of keeping overall prices low).

property rule. Under a property rule, users could well face a take-it-or-leave-it option between using the product and giving their personal information for free, or not using the product at all.[133] If they need to use the service, this consent would then not fully be given freely.[134] In addition, it would be difficult for an average Internet user to properly assess the risks of selling the right over her personal information.[135] Internet users generally face difficulties in assessing the risks of disclosing, because they do not always know how their data will be aggregated and what can be done with it—there is an information asymmetry problem.[136] The costs of assessing risks when selling rights over information would therefore be high.[137]

Information assembled by compiling different types of information provided by the Internet user to different companies at different times, called data mining, would be unprotected by property rules. The Internet user would have *ex ante* compensation for each piece of information released to each data collector.[138] However, she would not have *ex ante* compensation for the aggregated information, which is more valuable and, more importantly for the incentives to generate information, potentially more harmful.[139] Taken individually, these pieces of data might not be valuable enough to induce companies and Internet users to bargain over them,[140] but combined they present costs to users. People will lack incentives to incur risks

---

133. *Cf.* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1162 (1999) (describing the contractual elements of this relationship).

134. *Cf. id.* (stating that "the more the site seeks consent for collection and use of personal data, the more robust the firm's representations about the integrity of its data and the security with which it maintains the data").

135. *See id.* at 1128 (noting that some commentators think the law should supply corrective measures in these circumstances).

136. *See id.* at 1145 (explaining that data collection firms may gain broad access to a person's personal data).

137. *See id.* (adding that while most objects that are sold can be replaced, one cannot replace personal data once it is disclosed).

138. *See* Calabresi & Melamed, *supra* note 18, at 1092 ("Property rules involve a collective decision as to who is to be given an initial entitlement but not as to the value of the entitlement.").

139. *See* Samuelson, *supra* note 133, at 1138 (describing how some individuals might prefer their information not be shared with these later parties).

140. *See, e.g.*, Emily Steel et al., *How Much is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013, 8:11 PM), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz4a25NNzC3.

to disclose pieces of their personal data if they are paid very little for each of them while they face a high expected cost for them in aggregate.

Property rules over personal information could also introduce a principal-agent problem. If data collectors paid Internet users a price for their personal information, and those users were therefore already compensated, then data collecting companies would have no incentives to incur costs of care or to moderate activity levels (information processing) to avoid breaches.[141] The data collector would have full control over the information—which affects the Internet user's welfare—and incentives to over-process information and under-invest in care, increasing the risk of data breaches *ex post*.[142] This problem arises because property rules are satisfied only at the start, allowing the acquirer to forget about potential externalities later on—unlike liability rules, which can impose costs at all moments of the decision-making process.[143] Even if the expected externalities can be calculated into the price, companies have no incentives to take care *ex post*. For these reasons, even if property rules seem to provide a strong protection, they might not change the situation for Internet users significantly after all.

If users are rational, they will anticipate this increase in risk and, consequently, they would increase the price demanded for their personal information in accordance with those increased risks. This increase in the price of information produced by property rules would not necessarily be desirable for the aim of increasing the amount of information available. The price increase would reduce the demand for such information in equilibrium, which would reduce the supply of information to meet that demand.[144] In this way, property rules would fail to increase the amount of personal information available.

If property rules are traditionally suggested for scenarios with low transaction costs and Internet reduces the cost of

---

141. *See id.* at 1010–11 (suggesting that, despite earlier sentiments to the contrary, "it is [now] much easier than was previously assumed" to improperly use aggregated data to extract identifiable personal information).

142. *See id.*

143. This element has been considered a drawback of property rules, for example, in environmental law for the calculations of carbon dioxide emissions.

144. *See* Murphy, *supra* note 41, at 2385 (describing the "efficiency loss" associated with inhibited information disclosure due to higher cost).

communications (and therefore the cost of transacting, keeping all else stable), one could ask why property rules fail to accomplish their goals in the privacy context. Here we must recall that, for personal information, the cost of generating the good is the expected cost of a breach that can result from disclosure: the more personal information released, the higher the expected cost of a privacy breach. A property rule implies that the Internet user has to know the expected value of the data breach to ask for an equivalent price and be compensated *ex ante*.[145] From this perspective, a strict liability rule makes it easier to define expectations than does a property rule.[146]

Privacy breaches involve several potential parties who are unidentifiable ahead of time, many of whom only come into contact with the data *ex post*. For this reason, negotiating over one's information has high costs, even when communication costs are low. In turn, the disincentives for investment in the generation of personal information depend on the expected cost of breach—not the costs of a production process.[147] For this reason, the transaction costs of protection are more relevant than the transaction costs of communications to set a rule to protect privacy entitlements. This leads to considering the possibility of protecting data with liability rules.

C. A (STRICT) LIABILITY SYSTEM FOR PRIVACY

Liability rules for personal information—which would be similar to the privacy tort—would present a lower level of exclusion than would property rules. Under this rule, consent would not be a prerequisite for the transfer and Internet users would be unable to prevent a company from selling their

---

145. On the other hand, under a strict liability rule, if we assume perfect assessment, in case of a breach the Internet user would be compensated *ex post* with an amount that will leave her indifferent with respect to a non-breach situation.

146. *See generally* Ian Ayres & Eric Talley, *Distinguishing Between Consensual and Nonconsensual Advantages of Liability Rules*, 105 YALE L.J. 235 (1995) (arguing that liability rules are more efficient than property rules, even without prohibitively high transaction costs, when those transaction costs stem mainly from imperfect information) [hereinafter *Distinguishing Between Liability Rules*]; Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027 (1995).

147. *See, e.g.,* Murphy, *supra* note 41, at 2404 (illustrating an example of how the expected cost of a breach determines the value of the information at stake).

personal information to others, or from collecting their personal information. Still, the users would be compensated if any collection or processing resulted in harm, for example, by causing identity theft or the dissemination of embarrassing information.[148] Although this differs from the type of rules that most privacy advocates defend, it is a rule that, if effective, could leave Internet users as well off in the event of a privacy breach as in the event of no privacy breach. This should be taken into account to preserve their welfare and establish incentives for them to disclose.

A liability rule would allow for subsequent sales, thus keeping transaction costs low—this characteristic was one of the property rule's more attractive features.[149] The liability rule would also avoid the central problems identified for property rules: the latter rules' ineffectiveness due to asymmetric bargaining positions would be remedied by collectively defined prices in liability rules.[150] Fixing damages in accordance with the harm caused would solve the property rule's under-protection of information obtained through data mining.[151] Moreover, an *ex post* compensation would correct the principal-agent problem by varying compensation according to levels of care through liability.

Besides avoiding the problems generated by property rules, liability rules would present two advantages: one regarding conditions for harm and one regarding risk averseness. Regarding conditions of harm, people sometimes suffer no disutility from privacy unless they are aware of the data leak (subjective harm). In some cases of withholding data based on a pure privacy preference (irrespective of how others treat them after data are disclosed), utility is not reduced until Internet

148. *See* Ayres & Talley, *Distinguishing Between Liability Rules*, *supra* note 146, at 235 (agreeing that "liability rules can be more efficient than property rules when transaction costs are low").

149. *See id.* at 235 (claiming that "liability rules may also have a consensual advantage in low-transaction-cost settings (i.e., liability rules facilitate trade)").

150. *See id.* at 237 (stating that in terms of bargaining position, under Solomonic bargaining theory the "core insight was that dividing an entitlement between two negotiators could cause more forthright and efficient bargaining").

151. *See id.* at 236 n.3 (concluding that under a liability rule "even if damages are set imprecisely, liability rules can induce beneficial nonconsensual taking").

users become aware of other people's knowledge of that information.[152]

Two examples might clarify this point. On the one hand, someone might not want her insurance company to know about a medical condition because that could raise the premium, or she might not want her employer to learn about the traits that make her a less desirable employee. In those cases, she would suffer harm irrespective if she knew that they had the information. On the other hand, the same person might not want one's friends to know about a romantic comedy that she saw, or about online forums that she frequents, because she considers these embarrassing. In those cases, she would suffer harm only if she knows that her friends know about these activities. Harm based on pure privacy preferences is subjective harm: it refers to a psychological state rather than to external consequences.[153] Although this harm must also be taken into account, it materializes only when the Internet user is aware of the breach. This characteristic of privacy disutilities points to liability rules as a well-suited compensation mechanism, because in these situations there would be no welfare reduction without the entitlement-holder's knowledge, and hence no justification for an *ex ante* compensation mechanism.

The second advantage regarding risk attitudes is that, if Internet users are more risk-averse than data trading companies—which is likely—then liability rules could be in the interest of both players in the interaction even apart from their ability to solve the principal-agent problem.[154]

If the amount of *ex ante* compensation, such as that of property rules, is determined solely by the expected damage—independently of the disutility that people get from risk—full *ex post* compensation in the occurrence of damage would be more

---

152. This argument, however, has doubtful implications for data breach notifications: it could lead one to consider that data breaches should not be publicized when only this kind of information is involved. The conclusion is doubtful because there could be other overriding reasons to publicize, such as the difficulty in determining when the disutility is only of this kind, or the importance of reducing asymmetric information in processing.

153. *See* Calo, *supra* note 37; *see also* Murphy, *supra* note 41, at 2393 (arguing that it "is the subjective privacy preference that needs to be weighed against the value of the information").

154. *See* Calabresi & Melamed, *supra* note 18, at 1106 (explaining that risk may be reduced from a liability theory because a collective determination of value leads to quick and efficient transactions).

valuable for users than *ex ante* compensation.[155] On the other hand, if the compensation does take this into account and is higher than the expected damage to account for the disutility of risk—leaving Internet users indifferent between *ex ante* and *ex post* compensation—then a liability rule would be cheaper for data collectors than a property rule.[156] Under the most expensive case of strict liability, the rule's expected cost would not exceed the expected cost of harm, while under a property rule they would have to add to it a compensation for the disutility of risk.[157] This principle would be maintained even with a slight overcompensation, as long as the overcompensation was, in expectation, lower than the amount needed to cover risk averseness.[158] If liability rules are established when these risk attitudes are present, this is an argument in favor of an insurance policy that could take care of the disutility due to risk.

Last, we can ask which type of liability rule is the most appropriate for privacy. The situations in which IPL is involved are unilateral accidents, where the potential tortfeasors (data collectors and data processors) control the probability of an accident (data breach) and the extent of harm almost exclusively.[159] After data are disclosed, it leaves the Internet user's sphere of control, thereby rendering her unable to control it.[160] The protection mechanisms that Internet users can use after data are disclosed have a negligible influence on the probability of data breaches compared to the security measures that data processors can implement.[161] In addition, both the potential tortfeasors' care and activity levels are relevant for the

---

155. This assumes that the expected value of the damage is the maximum that companies are willing to pay, and that they would not compensate users for their risk averseness.

156. *Cf.* Murphy, *supra* note 41, at 2395 (reasoning that it is easier for a data collector to obtain permission when it wants to reuse information, than for the information creator to contract with all interested data collectors *ex ante*).

157. *See id.*

158. *See, e.g.*, *id.* at 2397 ("An activity that may generate embarrassment or reprobation from some sectors of society will not occur if the activity carries with it a significant risk of being disclosed.").

159. *See* Chris Jay Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J.L. & TECH. 1, 33 (2009) (explaining that "database providers have ultimate control over use of personal information and protections that are in place").

160. *See id.* at 1 ("One faction explains the identity theft as a problem of a lack of control over personal information.").

161. *Id.*

accident's probability.[162] The level of database security (care level) and the number of data transfers performed by data collectors and data processors (activity levels) directly affect the probability of data breaches.[163] Therefore, it seems that, among the different possible liability rules, a strict liability rule would induce appropriate levels of care and activity most efficiently.[164]

D. LIMITATIONS OF LIABILITY RULES IN IPL

The central drawback of this liability rule is the large information cost that it would entail, which might render it inapplicable despite its theoretical benefits. If an Internet user faces harm due to a privacy breach (for example, because her identity is stolen) it might be unclear which company or group of companies that held her personal information suffered a data breach that, in turn, led to such outcome. Causality could be difficult, if not impossible, to prove. This leads to the question of whether this difficulty could be solved by using a model of causal uncertainty with multiple tortfeasors, as is sometimes done with environmental harm where responsibility is apportioned inversely to levels of care.[165]

Causal uncertainty is a challenge for those types of responsibility within tort law for which it is difficult to determine the source of damage, such as environmental harm and medical malpractice.[166] To some degree, privacy is

---

162. *See id.* at 33 (noting that "[d]atabase operators constitute the cheapest cost avoiders vis-à-vis individuals whose information sits in a private entity's database").

163. *See id.* ("The relationship is so asymmetric that the individual is literally at the mercy of the risk preferences of companies with which no relationship has even been established.").

164. *See id.* at 32–35 (suggesting strict liability for identity theft); *see also* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 261–68 (2007) (reporting that the application of a negligence rule to databases for personal information leakage has been attacked on the basis that uncertainty would surround the level of due care, leading databases to overinvest in care). But note that a negligence rule with an ambiguous standard would lead potential plaintiffs to overinvest in care only up to the investment level they would have under a strict liability rule, and this is a socially efficient level of care for unilateral accidents because it would fully internalize the externalities imposed.

165. Marcel Kahan, *Causation and Incentives to Take Care Under the Negligence Rule*, 18 J. LEGAL STUD. 427, 430 (1989) (describing a model where care and expected costs of accidents share an inverse relationship).

166. *Id.* at 440–41.

analogous to these. In this context, there are two different types of causal uncertainty problems. The first is whether any of the defendants caused the harm, and the second (conditional on a positive answer to the first) is who among them hurt the plaintiff and how much.[167]

When the first question is answered, and causal uncertainty appears for the second, the problem is reduced to matching each victim with her tortfeasor.[168] In these cases, market-share liability is a solution under the assumption that the marginal increase in the risk of harm created by each defendant to each victim is proportional to its presence in the market. Under this assumption, the marginal increase of risk to the potential victims will be equal to the firm's market share. For the assumption to be verified, potential tortfeasors must have similar care levels and they must have activity levels proportional to their market shares.

This assumption seems to hold in the leading market share liability case *Sindell v. Abbott Laboratories*,[169] where market share liability removed from victims the burden of proving which among the drug producers that harmed them as a group harmed each of them individually.[170] The assumption also seems appropriate in cases of recurring harms between parties.[171] Even though these situations present some degree of uncertainty concerning the identity of the tortfeasor for each victim, the uncertainty over tortfeasors in the aggregate is low because the marginal increase in the risk of damage for the entire set of plaintiffs is (considered) proportional to market share.[172]

---

167. David Rosenberg, *The Causal Connection in Mass Exposure Cases: A "Public Law" Vision of the Tort System*, 97 HARV. L. REV. 849, 855–57 (1984).

168. Saul Levmore, *Probabilistic Recoveries, Restitution, and Recurring Wrongs*, 19 J. LEGAL STUD. 691, 697–98 (1990).

169. 607 P.2d 924 (Cal. 1980). In the case, pregnant mothers used a diethylstilbestrol-based drug (DES) to prevent miscarriage, which caused their daughters (later on known as "the DES daughters") to develop cancer twenty years later. In the DES cases this assumption is reasonable because all defendants engaged in an identical activity. *See* Glen Robinson, *Multiple Causation in Tort Law: Reflections on the DES Cases*, 68 VA. L. REV. 713, 722 (1982).

170. *Sindell*, 607 P.2d at 936–37.

171. Levmore, *supra* note 168, at 697.

172. *See generally* William Kruskal, *Terms of Reference: Singular Confusion About Multiple Causation*, 15 J. LEGAL STUD. 427 (1986); William Landes & Richard Posner, *Joint and Multiple Tortfeasors: An Economic Analysis*, 9 J. LEGAL STUD. 517 (1980).

The assumption that the marginal increase in the risk of harm created by each defendant to each victim is proportional to its presence in the market, however, is rarely valid for companies collecting and processing personal information. Personal information trades do not always have a negative impact on Internet users' well-being. The trade of information is sometimes harmless and, when it is not, the possibility that it presents of creating harm largely depends on care levels. The type of uncertainty problem that appears for privacy is not the matching problem between individuals from a pool of plaintiffs and individuals from a pool of defendants, but the more general uncertainty of the wrongdoers' identity.

This problem was addressed by laws that require companies to notify their customers in the event of data breach—such as the *Personal Data Notification and Protection Act* introduced in Congress in 2015[173]—which marginally reduce the information problem. However, other problems remain for market share liability to succeed in privacy. Victims of fraud or identity theft do not always know how their data were leaked, and by whom. Sometimes the set of necessary data is not even leaked from one single place but elements of that set are mined from different sources, making an efficient apportioning of responsibility increasingly difficult.[174] Moreover, an additional difficulty in applying this market-share approach arises because companies constantly enter and exit the market—as is often the case in information technology. Finally, the rule works when the possible sources of harm operate at the same level—for example, when they are all data collectors. If companies operate at different levels, then they operate in different markets, and apportioning liability becomes more difficult.

Additionally, in the context of information technology, several websites have a small market share compared to data giants, but they still process large amounts of personal information.[175] This asymmetry could lead to the inapplicability of market-share liability while potentially leaving some scope for using another proxy for apportionment, such as the amount of

---

173. Personal Data Notification and Protection Act of 2015, H.R. 1704, 114th Cong. (2015). These protections currently exist at state level.

174. Hoofnagle, *supra* note 159, at 31–32.

175. Catherine Tucker, *The Economics Value of Online Customer Data*, at 2.2 (Org. for Econ. Cooperation & Dev., Background Paper No. 1, 2010), https://www.oecd.org/sti/ieconomy/46968839.pdf.

data collected or data traded. This alternative, however, would lead to frequent solvency problems because many of these companies have large datasets but few assets, and they would be unable to fully compensate people for their losses. These companies could be judgment-proof. Mandatory insurance could be required to address this problem, but it would increase costs and decrease the number of players in the market because those who could not afford the increase in costs would fall out.

Last, there is an uncertainty problem that goes beyond the causal problem: there are transaction costs in the valuation of the harm that, in light of the problems mentioned for market share liability, can be significant. Whoever the deciding body for the value of the harm is, it will have to incur costs that should be computed when deciding whether to apply a liability rule.

V. HOW PRIVACY LAW CAN FOSTER INFORMATION

A. DETERMINING IPL'S MIXED PROTECTION

The last part's central lesson is that IPL should set a level of exclusion that varies depending on context, and should in general be higher than liability rules, but lower than property rules or inalienability rules. All three types of rules applied by themselves would present either theoretical or practical problems that could undermine them as protection mechanisms.[176] This fits Calabresi and Melamed's observation that the same object can be protected by different rules depending on circumstances,[177] and it leads to the question of how to combine them to protect personal information under IPL. We can ask, along these lines, if there are other areas of the law that do this, in order to find guidelines in them to construct the best possible set of rules.

The rationale of limiting access to information by third parties to incentivize personal information disclosure is used canonically to justify professional confidentiality.[178] Most societies want to ensure that people are able to convey as much

176. *See generally* Calabresi & Melamed, *supra* note 18 (discussing the theoretical frameworks of the three rules).

177. *Id.* at 1105–06.

178. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 123 (2007) (stating that American law parted from the idea of privacy as confidentiality, while English law maintains a notion of privacy that focuses on trust within relationships).

information as possible to their fiduciaries (lawyers, psychologists, priests) so they can perform appropriately in their jobs.[179] For that reason, law and professional codes of conduct prohibit members of these professions from disclosing information shared with them in the performance of their duties, thus guaranteeing trust.[180] A confidentiality rule preventing members of these professions from learning the information in the first place would be too protective and would impair the rule's aim. In turn, a rule that allows them to disclose everything their clients say, analogous to no privacy, would make their clients disclose less, if anything at all.[181]

This has been the justification for the attorney-client privilege.[182] Privilege is not considered the attorney's right but rather the client's, and she can decide whether to raise it or waive it; privilege has on occasion been explicitly called a rule of privacy.[183] The extent of the privilege is that attorneys cannot disclose information without the client's permission. In a narrow interpretation, this includes any information conveyed in confidence with the purpose of seeking legal advice;[184] in a broad interpretation, it includes any communication between attorneys and their clients.[185] Its justification is that attorneys can give better legal advice if they know all relevant information and, absent privilege, clients might withhold information.[186]

---

179. *See* Ronald J. Allen et al., *A Positive Theory of the Attorney-Client Privilege and the Work Product Doctrine*, 19 J. LEGAL STUD. 359, 371–72 (1990) (noting that "Wigmore's idea that the privilege is needed to ensure full disclosure [is] still the dominant theme in the literature").

180. *Id.*

181. *See* Murphy, *supra* note 41, at 2406 (noting that even "merchants may prefer privacy in many instances, because a rule favoring privacy encourages truthful communication").

182. The original justification appears in Wigmore's leading book on evidence. JOHN WIGMORE, WIGMORE ON EVIDENCE § 2291 (1940) ("In order to promote freedom of consultation of legal advisers by clients, the apprehension of compelled disclosure by the legal advisers must be removed . . . .").

183. *See* Geoffrey Hazard, *A Historical Perspective on the Attorney-Client Privilege*, 66 CALIF. L. REV. 1061, 1062 (1978).

184. *See* FED. R. EVID. 501.

185. *See* MODEL RULES OF PROF'L CONDUCT r. 1.6 (AM. BAR ASS'N 2006).

186. *See* Allen et al., *supra* note 179, at 372; *see also* EDNA EPSTEIN, THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE 4 (4th ed. 2001) ("With fear of disclosure, all facts will not be freely revealed and legal advice cannot be effectively given.").

However, while attorney-client privilege is analogous to IPL in its aims to stimulate disclosure, it is not the most useful guideline to determine good privacy rules for other contexts. In speaking only to the attorney-client communication, it does not address the full range of problems that IPL must grapple with. Privilege does not present the problem of information's future use and of information's secondary use and data transfers, which are essential to information's public good characteristic.

Another branch of law that displays a combination of liability and property rules to stimulate the creation of content is copyright.[187] Copyright law, in addition, must also deal with the public good characteristics of information and its secondary use. It responds to the non-excludability characteristic of information and to the need to foster it with the creation of an entitlement that excludes others from some uses, while at the same time it attempts to maintain low transaction costs for the information's transfer and future use.[188] Concretely, copyright law reserves for authors some property rights, mainly the right to exclude others from copying.[189] IPL, from the economic perspective in which it was presented, has relevant analogies with copyright inasmuch as they both present some level of exclusion but do not solely consist on property rules.[190] Copyright, therefore, serves as a better guideline.

B. IPL AND COPYRIGHT: COMMON GROUNDS

In their seminal article, Warren and Brandeis already relate privacy to copyright law.[191] Copyright seeks to balance competing interests in the creation and dissemination of creative

---

187. *Cf.* Hardy, *supra* note 63, at 218 (noting that copyright is "only one of several incentives that encourage the production of informational works").

188. *See* Besen & Raskind, *supra* note 108, at 3, 14–15.

189. *Id.* at 12. As manifestations of copying, copyright law traditionally grants five rights: (i) the right to reproduce, (ii) the right to prepare derivative works, (iii) the right to distribute copies, (iv) the right to perform, and (v) the right to display the work publicly. In the United States, this is codified at 17 U.S.C. § 106 (2012).

190. Hardy, *supra* note 63, at 232.

191. They based their claim on rights granted by the common law to "each individual . . . of determining ordinarily, to what extent her thoughts, sentiments, and emotions shall be communicated to others." Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198, 199–202, 208–11 (1890).

works.[192] A price higher than the marginal cost of distribution (which for digitalized information is zero) generates the dynamic effect of incentivizing the generation of new works. This dynamic effect is weighed against the static effect of suboptimal dissemination.[193] Authors' protection is mainly given by the property characteristics of copyright, which imply compensation, while the attempt to maintain dissemination leads to the (few) liability characteristics of copyright. From the perspective proposed in the last section—IPL as an instrument to incentivize the creation of information—copyright law and IPL have similar justifications. Moreover, they have a similar way of combining property and liability rules. Neither copyright law nor IPL typically include inalienability rules.[194]

Regarding the property characteristics of copyright law, authors holding copyright are entitled to exclude others from copying their work.[195] The holders are able to either transfer copyright in its entirety or (more frequently) grant a license for the use of their work in exchange for a royalty,[196] partially alienating their exclusion right, and to request injunctions for the breach of such exclusion.[197]

While in real property, entitlements are often transferred in their entirety—meaning the new owner can do with it what she desires.[198] In copyright, the copyright holder usually gives

---

192. *See* Joseph Liu, *Copyright and Time: A Proposal*, 101 MICH. L. REV. 409, 429 (2002); Glynn Lunney, *Reexamining Copyright's Incentives-Access Paradigm*, 49 VAND. L. REV. 483, 492–93 (1996).

193. Besen & Raskind, *supra* note 108, at 16 (giving as an example the need to get permission for the creation of derivative works).

194. *But see* Hardy, *supra* note 63, at 229–30 (identifying the inalienability aspect associate with copyright's prohibition on bargaining away the right of termination). Another exception is the author's termination right, which gives authors the right to terminate an assignment decades later, operating as a *de facto* inalienability rule.

195. *See generally* WILLIAM CORNISH, DAVID LLEWELYN & TANYA APLIN, INTELLECTUAL PROPERTY: PATENTS, COPYRIGHT, TRADE MARKS AND ALLIED RIGHTS 1–41 (2013); BJ Ard, *More Property-Like than Property: The Prevalence of Property Rules in IP* (SSRN Elec. Library, Working Paper No. 2,811,932, Sept. 29, 2016), https://ssrn.com/abstract=2811932.

196. *See* CORNISH ET AL., *supra* note 195, at 525–30.

197. *Id.* at 72; *see also* Ard, *supra* note 195, at 30 (arguing that copyright statutory damages awards are often high enough to function as property rules).

198. However, not all tangible property transfers are in fee simple (though most chattel transfers are). For example, I can grant a limited easement for a neighbor's passage over a certain part of my land without transferring ownership; I can grant a time- or activity-limited license for entry to my land,

permission for a particular use—the holder can state the purpose.[199] In this regard, licenses under copyright law are somewhat analogous to the purpose limitation principle under European Data Protection Law (DPL), according to which information cannot be processed in a way incompatible with the purposes for which it was collected.[200] Both of them specify the objective for which the information can be used and forbid its use for other purposes.[201] They are an element of a property rule within the system, where the entitlement-holder has the right to exclude others from uses different than the one specified.[202] The difference between them is that in copyright, the entitlement-holder over the original data sets the purpose in drafting the license, while in IPL the individual who generates the data does not. Instead, the transferee (data collector or processor) makes this decision, even if in some systems such as European DPL she is not completely free in doing so but must remain within an established legitimizing purpose.[203]

Under both copyright (or, more generally, under intellectual property law) and IPL, each type of information should ideally have a different protection to incentivize it without overprotecting it, but it is too costly for the law to account for all nuances.[204] An ideal intellectual property law in a world with perfect information would have a different scope and breadth for each creation. As this is not possible, however, the law uses categories that aim to provide the appropriate level of protection on average. Namely, intellectual property systems feature standard protections for patented inventions and standard protections for copyrighted works.[205] IPL faces the same issue:

---

making anyone who exceeds that license a trespasser; and I can make a conditional transfer such that the owner forfeits her rights if she violates the condition.

199. *See generally* CORNISH ET AL., *supra* note 195, ch. 13.

200. *See* Council Directive 95/46, art. 6(1)(b), 1995 O.J. (L 281) 31, 40 (EC).

201. *See* CORNISH ET AL., *supra* note 195, ch. 13.

202. *See* Calabresi & Melamed, *supra* note 18, at 1092.

203. EU Data Protection Law lists different means by which someone can legitimately collect or process personal information, the most important of which is consent from the user to whom the information relates. Other bases are compliance of a legal obligation and public interest. *See* Council Directive 95/46, art. 7(a), 1995 O.J. (L 281) 31, 40 (EC).

204. *Cf., e.g.*, Pierre Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1105–06 (1990) (discussing the difficulty of applying the "fair use" standard to different types of copyrighted material).

205. *See generally* Besen & Raskind, *supra* note 108.

the expected cost of disclosing is different for each type of information and for each Internet user. Although it would be ideal to de-homogenize information and have individual rules, the information cost of this and the transaction cost of administering the system would be too high. IPL has distinctions that aim to work on average, for example between sensitive and non-sensitive information.[206] Depending on how finely the law defines types, the costs would also vary within each type as well.

Regarding copyright's liability characteristics, authors face some compulsory licenses and have to accept fair use.[207] While compulsory licenses tend to be specific and limited, fair use is a central trait of copyright law.[208] As such, while fair use could marginally reduce the number of works created, it represents an advantage for the dissemination of copyrighted works, balancing the incentive objective and the access objective mentioned earlier.[209] Like liability rules under the Calabresi-Melamed framework, fair use is justified by high transaction costs. Specifically, by the high transaction costs that would otherwise be incurred in negotiating and monitoring the uses that it protects.[210] For example, the law allows to quote a scientific work without the author's permission because obtaining such permission every time would create exceedingly high transaction costs, while citations do not harm the author's economic interest.[211] If the quotation is large enough to cover and thereby substitute for the whole work, on the other hand, it would harm the author's economic interest, and the law requires permission to do so.[212] It would be unjustified to ban use when such ban

206. *See, e.g.,* Personal Data Notification and Protection Act of 2015, H.R. 1704, 114th Cong. (2015).

207. Hardy, *supra* note 63, at 233; Ard, *supra* note 195, at 32–36 (describing the liability rule features of copyright).

208. This is particularly so in the United States. *See* 17 U.S.C. § 107 (2012).

209. *See* Leval, *supra* note 204, at 1110; Glynn S. Lunney Jr., *Fair Use and Market Failure:* Sony *Revisited*, 82 B.U. L. REV. 975, 981–82 (2002).

210. Wendy Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the* Betamax *Case and Its Predecessors*, 82 COLUM. L. REV. 1600, 1618 (1982).

211. In expectation, they do not reduce the expected number of copies sold—in fact, they may increase sales.

212. In general, fair use finds its scope defined in the uses of the product that do not significantly affect the economic interests of the owner and, as a doctrine, strives to prevent the stifling of creation. *See* Leo J. Raskind, *A Functional Interpretation of Fair Use: The Fourteenth Donald C. Brace Memorial Lecture*, 31 J. COPYRIGHT SOC'Y 601, 618 (1983) (noting that copyright

would not induce a negotiation, and so generate a loss by leaving the author uncompensated and the user without access. Fair use, in this sense, is a tool to enhance the diffusion aspect of copyright law.[213]

The same argument can be made for IPL. Demanding authorizations from the Internet user for each secondary use of information would significantly increase transaction costs, especially given that personal information is valuable when aggregated, and that information processing involves a large number of Internet users. To avoid this consequence, IPL presents liability rules within the scope of the purpose limitation principle by not requiring consent for every interaction.[214]

Creating entitlements over personal information, and particularly the analogy with copyright or other intellectual property rights, has been argued before to present difficulties.[215] In a thoughtful article, Samuelson has argued that establishing a "property right" (entitlement with a property rule) over personal information would mean, in essence, creating a new intellectual property right.[216] But this right, Samuelson argues, would generate an incompatibility between the reasons to protect information with intellectual property law and the reasons to protect personal information.[217]

In Samuelson's words,

> [t]he economic rationale for intellectual property law arises from a public goods problem with information products that this law strives to overcome. In the absence of intellectual property rights, there may be too little incentive to induce an optimal level of private investments

---

holders must "prove either a present or a potential economic injury to the value of the copyrighted property" to challenge use of the property). *See generally* Richard Posner, *When is Parody Fair Use?*, 21 J. LEGAL STUD. 67 (1992) (discussing the level of infringement upon the original source that should be allotted to parodies under the fair use doctrine).

213. *See* Gordon, *supra* note 210, at 1613.

214. *See* Council Directive 95/46, art. 7(b)–(f), 1995 O.J. (L 281) 31, 40 (EC).

215. Samuelson, *supra* note 133.

216. *See id.* Other objections to the propertization of personal information, such as the difficulties of alienability, are also present in the article. These objections are included in Section III.C, pertaining the difficulties of a property rule. This conceptual objection, however, must be treated separately, because it concerns the entitlement, and not merely the protection rule. *See supra* Section III.C.

217. Samuelson, *supra* note 133. An earlier version of this argument is available in Rochelle Cooper Dreyfuss, *Warren & Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8 (1999).

> in the production and dissemination of intellectual products . . . . The prospect of being unable to recoup research and development costs may deter such investments from being made in the first place. A limited grant of property rights in intellectual productions gives creators assurance that they can control the commercialization of their work and enjoy some fruits of their labor . . . .

The standard rationale for granting property rights in personal data is, of course, quite different.[218]

The considerations made in Part II contest the objection that the law should not protect personal information with a system analogous to copyright because the two fields are based on different justifications. Both IPL and copyright promote the generation of information, and have further common grounds in the way that, to do so, they combine property and liability rules.[219]

C. IPL AND COPYRIGHT: STRUCTURAL DIFFERENCES

There are also, however, structural differences between the activities affected by copyright law and IPL that justify different treatments.

The first of these differences is that the cost of creating a copyrighted product does not depend solely on its use *ex post*, while the cost of disclosing personal information fully depends on how it is used after the exchange—because this use determines the expected cost of harm. For most copyrighted works, the central costs are those of creating the work and creating copies.[220] However, for disclosing personal information, the costs are the expected cost of harm that people face when disclosing information (instrumental value of privacy or objective privacy harm), and the disutility of the information disclosure in itself (pure privacy preference or subjective privacy harm).[221] In both cases, for the good to be produced the expected return must exceed the expected cost, but for one of them (IPL)

---

218. *See* Samuelson, *supra* note 133, at 1139–40 (footnotes omitted).

219. See *id*. at 1134 (stating that "[i]ntellectual property law grants exclusive rights in information-based creations in order to promote development . . . of information and a creation of new property rights seems almost inevitable").

220. *See, e.g.*, Landes & Posner, *supra* note 58, at 336–39. One can also imagine other costs, such as the use of the material in a way that reflects poorly on the creator.

221. Calo, *supra* note 37, at 1141–43 (distinguishing between objective and subjective privacy harms).

the cost depends almost exclusively on the *ex post* incentives for others to adjust levels of care and of activity. Because liability rules maintain *ex post* incentives better than property rules, this justifies a stronger incidence of liability rules in IPL than in copyright.

A second difference between copyright and IPL is how the value of information changes over time. The limited duration of copyright responds to its length's decreasing marginal utility paired to its increasing marginal cost.[222] Information under IPL also has, in most cases, decreasing marginal utility of length of protection for the creator. A leak of old personal information tends to harm Internet users less than one of new information—even disclosures of undesirable acts are worse when the act is recent than when it is not. However, regarding marginal cost, unlike copyrighted work, personal information becomes less valuable over time as well for others. While the reputational value of personal information seems to decrease at a relatively slow rate for Internet users, it quickly decreases in value for its commercial uses as it becomes outdated.[223] Moreover, due to the higher incidence of liability rules in IPL compared to copyright, tracing the information creator to allow for secondary use once transferred is unnecessary: companies typically do not need consent to transfer information to third parties—and even when they do, they can obtain consent in advance at the time they collect the information.

Policy debates about IPL have proposed to increase protection for old information when compared to new information, having gone in the opposite direction from copyright's time limits.[224] However, although not explicitly, IPL also contains a time limit for its entitlements—the Internet user's death—because, unlike copyright, data-protection rights

---

222. Regarding marginal utility, prospective authors whom the law seeks to incentivize will discount payoffs to present value. Regarding marginal costs, this is mainly due to tracing the origins of old copyrighted works. *See id.* at 361–63.

223. For an example of this, see Costeja's claim in Case C-131/12, Google Inc. v. AEPD, 2014 E.C.R. 1.

224. An example of this is the right to forget. *See generally* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009) (discussing the permanence of information in the digital age and arguing for implementing steps that allow the Internet to "forget").

are not inheritable.[225] The difference in the value of information over time mentioned in the last paragraph can justify the different time limits in the two branches of law. After the death of the Internet user, personal information has, on average, less value for her heirs than it did for her. This can justify its non-inheritability even within the tendency of giving further protection to older information.[226]

The two branches of law do present differences that can explain why IPL should not be (and is not) subsumed under copyright law.[227] This presents a partial agreement with Samuelson's argument.[228] While, under the argument of this paper, it would be an overstatement to argue that there are no common underlying reasons to protect copyright's creations and IPL's personal information, the differences are large enough to require two separate branches of law to treat them, and personal information cannot be just another intellectual property right. Even if we can, and we should, protect personal information in a system analogous to copyright law, we should not protect it with copyright law directly.[229]

These considerations point to an economic justification for having within IPL a system similar to copyright with a combination of property and liability rules, where only some rights from the bundle (as property is often characterized) are reserved.[230] As with Creative Commons, which proposed a successful model to protect creations with a lower level of exclusion than traditional copyright law, we should discuss

---

225. Edina Harbinja, *Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives?*, 10 SCRIPT-ED 19, 35–36 (2013).

226. This effect varies, of course, depending on the reputational effects that the information has on heirs, and it has exceptions, such as genetic information about hereditary conditions.

227. *See* Samuelson, *supra* note 133, at 1141 ("Given the mismatch between the purposes of personal data protection and of traditional intellectual property rules, it would be difficult to justify such legislation under . . . copyright and patent legislation.").

228. *See id.*

229. This relates to the objection, also advanced by Samuelson, that including personal information as intangible property would lead to incoherence of intellectual property law. *See id.*

230. *See id.* at 1129 (stating that "[d]eep differences in the purposes and mechanisms of traditional intellectual property rights regimes . . . raise serious doubts about the viability of a property rights approach and about its prospects of achieving information privacy goals").

which rights of the bundle are worth keeping to protect personal information.[231] The next section addresses this question.

D. TREATING DIFFERENT TYPES OF INFORMATION DIFFERENTLY

So far we have seen the reasons to create privacy entitlements, and the different ways to protect them. An additional point follows from the information production argument: that different types of information ought to be protected in different ways.[232] Some technological characteristics of information exchanges, which have consequences for production, provide additional considerations to improve IPL from an economic perspective. The main elements for these purposes are three: on the supply side, the generation of information and its externalities, and on the demand side, the uses that can be given to it.

On the supply side, to incentivize information production, we must identify how it is created. Copyright's property characteristics attempt to prevent freeriding on the author's expression, thereby internalizing the positive spillovers.[233] The same rationale should be applied to IPL, protecting some types of data more than others.

Concretely, from this perspective, a higher level of protection is justified for information generated based on the user's consent. This is analogous to the economic rationale of copyright law for protecting expression but not ideas, because (i) ideas expressed by others is information that had significant input from someone else, (ii) protection of ideas would be too wide and would likely compensate creators beyond their costs, and (iii) this would elevate transaction costs.[234] Only information generated based on the user's consent fits within peer-to-peer sharing, where Internet users produce the information to the degree to which their expected costs are

---

231. There are additional rights, other than property rights, that may make it possible to protect personal data. *See, e.g.*, *id.* at 1146 ("[I]t may be worth mentioning 'moral rights' of authors as a model for a nontraditional property right that might be adaptable to protecting personal data.").

232. *See, e.g.*, BJ Ard, *Confidentiality and the Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries*, 16 YALE J.L. & TECH. 1 (2013) (detailing a regime to protect reading records).

233. *See* Landes & Posner, *supra* note 58.

234. *Id.*

compensated.[235] Therefore, this type of information should be given a higher level of protection than the rest to incentivize its generation.

For example, Google Earth has significant marginal costs of gathering information—by taking pictures across the globe—while Google+ and other social networks do not, because they form part of a system where people surrender information voluntarily.[236] Both products fall roughly under the same privacy rules,[237] but Google Earth's methods of gathering information are closer to those that traditional privacy law deals with.[238] To incentivize information generation, users' privacy should have a higher level of protection for Google+ than for Google Earth.

From this perspective, the under-protection of privacy related to data mining (mentioned as a drawback of the property rule) could be welfare enhancing.[239] Data mining implies costs of assembly for the data miner, who after such process generates new information by combining the pieces of information used. If personal information generated by data mining were granted a lower level of protection than personal information acquired in its entirety, IPL would incentivize the generation of new information via data mining as well. Some level of protection should still be granted because, even if the data miner added value, she did not create the information from nothing, but needed individual pieces of data to construct it.

This leads to the more general question of who owns, under the property elements of IPL, information that was generated by someone other than the information's subject. Under current IPL, to the extent that it features property characteristics, the information's initial owner is the person whom the information concerns (the Internet user).[240] To incentivize information production, however, some property interests should be granted

---

235. *See* discussion *infra* notes 237–39.

236. *Compare* GOOGLE EARTH, https://www.google.com/earth/ (last visited Feb. 8, 2017), *with* GOOGLE+, https://plus.google.com/ (last visited Feb. 8, 2017).

237. Jurisdictional issues notwithstanding.

238. *See Earth Help*, GOOGLE, https://support.google.com/earth/answer/6327779 (last visited Feb. 8, 2017) (explaining how Google Earth images are collected).

239. *See generally* Hagel & Rayport, *supra* note 84.

240. *But cf.* Prins, *supra* note 42, at 276 (explaining that on social media profiles, the social media organization owns the personal information disclosed on profiles).

to the information's creator in scenarios where she is not the person to whom the information refers. This information-creator has different production and cost functions than Internet users who disclose data. For the former, personal information is not a by-product, and the costs associated with it are unrelated to expected privacy breaches.[241] But, inasmuch as IPL serves to incentivize information production, the cost of generating such information should be compensated as well.[242] Following the previous argument, the more the added value of the company to produce a piece of information, the more IPL could reduce the level of protection when compared to the situation in which the user generates the information by herself. It is difficult to imagine a case in which a company can produce personal information about a user without any help from her—which means that some level of protection should always be present.

An analogy can be drawn with the way intellectual property assigns interests. For instance, rights over photographs are assigned to the author (the collector of information) as opposed to the person photographed, and she is entitled to use it without the consent of the person who was photographed—with some limitations such as those imposed by the subject's right to publicity.[243] This rule incentivizes the generation of photographs (which are one kind of information) because it allocates the entitlement to the actor who needs to make the larger marginal investment for the photograph's creation.[244]

The second consideration, again from the supply side, is the cost to Internet users of producing information. To determine the expected cost that a user would face from disclosing a piece of information, it becomes relevant again whether it was generated based on consent. From the point of view of revealed preferences, information that a user decided not to reveal is more likely to present a larger expected cost for her than information that she chose to reveal. There could be, from this perspective, a self-

241. *See* Hagel & Rayport, *supra* note 84.

242. This property interest would be relevant, for example, for journalism. At a more general level, this principle would play a role in maintaining freedom of expression within IPL.

243. *See* Prins, *supra* note 42, at 283 (discussing the arguments surrounding the right of publicity).

244. *See* Samuelson, *supra* note 133, at 1150 (explaining that "publicity law largely concerns itself with providing appropriate incentives to induce investments in creative efforts, not to protect personality based interests").

selection process where undisclosed data presents higher risks. Here consent would seem to operate in the opposite direction than before: the less consent involved, the more protection needed. However, when personal information is a by-product, this is not necessarily true: there can be information that an Internet user did not have incentive to disclose, not because it has a high expected cost, but because it has a low expected benefit.[245] In the example given before, maybe she does not care about disclosing her location, but she gets no utility from fitness applications.

A better indicator than consent to determine the level of externalities is the type of information disclosed. There are different levels of privacy risks between sensitive and non-sensitive data, and between online and offline data. We could presume that the non-disclosure of sensitive data is motivated by the self-selection process mentioned above and therefore disclosing is potentially harmful, while the non-disclosure of non-sensitive data might be due to lack of incentives to disclose.[246] Under this assumption, less consent involved would mean more privacy protection needed only for sensitive information.

Both of these elements (consent and type of data), and to some extent the assumption regarding the differences between undisclosed sensitive and non-sensitive data, are present in IPL. In the United States, different statutes provide an increased level of protection to different kinds of information considered sensitive, such as the Health Insurance Portability and Accountability Act (HIPAA) for medical data and the Fair Credit Reporting Act (FCRA) for personal credit information.[247] European DPL, gives special protection to sensitive data more

---

245. Companies combat this low-benefit obstacle by offering incentives to users that disclose personal information. *See* Prins, *supra* note 42, at 277 ("One example of such a benefit is offered by . . . [the] Google Gmail initiative: it offers greater storage space in return for having Google monitor email and use the information for advertising.")

246. It is not easy to determine which information is sensitive, and which is not. The United States does not have a general statute that defines sensitive information. A general approach could consider information that could lead to discrimination as sensitive. European DPL has an enumeration of types of information considered sensitive, such as age, race, and gender.

247. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (1996); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012).

directly through the rule that, unlike other kinds of data, it can be processed only on the basis of consent.[248] Non-disclosed sensitive data, in this way, has a protection closer to a property rule, reflecting the different levels of expected externalities.

On the demand side, we should distinguish what use can be made of the information, because not all types information have equal social weight. On average, less social gain might be extracted from information that can be used solely for marketing (and might represent, individually, a low benefit for the company) compared to information that can be used for research regarding public health or the prevention of crime.[249]

It would be impossible for IPL to assess each unit of information individually to provide a tailored level of protection.[250] However, a plausible heuristic to approximate the social value of the information's use, and the level of internalization of this value, is whether its use serves a public good or a private interest.[251]

This distinction has already been taken into account to a limited degree by the law. European DPL does so by incorporating exceptions for freedom of expression,[252] research,[253] and healthcare,[254] where the Internet user has a lower level of protection.[255] The U.S. sectoral approach seems to attempt this as well, with tailored exceptions and provisions for its specific statutes, such as HIPAA's permitted uses and disclosures of personal without patient consent for treatment

---

248. *See* Council Directive 95/46, art. 8(2)(a), 1995 O.J. (L 281) 31, 40–41 (EC).

249. *See* Prins, *supra* note 42, at 273 (noting that crime detection is one of the useful results of our data-based society).

250. *Cf. id.* at 300 (stating that new technologies may enable the provision of individually tailored services).

251. *See* J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PA. L. REV. 875, 882 (1999) (stating that "[w]hile legislative adoption of our proposed doctrinal safeguards would enable entrepreneurs to preserve the benefits of Article 2B [of the UCC] . . . it would discourage them from . . . undermin[ing] essential public good uses of information").

252. *See* Council Directive 95/46, art. 9, 1995 O.J. (L 281) 31, 41 (EC).

253. *See* Council Directive 95/46, art. 6(1)(b), 6(1)(e), 11(2), 13(2), 32(3), 1995 O.J. (L 281) 31, 40–42, 49–50 (EC).

254. *See* Council Directive 95/46, art. 8(3), 1995 O.J. (L 281) 31, 41 (EC).

255. Note that the directive defines these exceptions broadly, for countries to have a broad scope of discretion in their implementations.

purposes—applicable when a provider needs record access to ensure quality care.[256]

The problem with the omnibus approach is that it makes it more difficult to distinguish between uses and between types of information. The problem with the sectoral approach is that the industry-specific statutes protect different channels of data flow, not different types of information, which map onto the different private interests, or of uses, which could be used as a proxy for social value.[257] HIPPA, for example, protects health data collected by doctors and insurers but not by commercial devices, which continue to become pervasive.[258] The Gramm-Leach-Bliley Act (GLBA) applies only to some financial institutions, as defined in the same statute.[259] The Video Privacy Protection Act (VPPA) applies only to physical recordings and not to online video streaming,[260] which is arguably more relevant. The Stored Communications Act (SCA) applies to text messaging but not to social media postings.[261] Still, while these are industry-specific and not information-specific, there is some correlation between industry and type of information involved regarding private interests and uses.

This mixed protection approach is able to justify IPL's central elements, and in particular the rights that Internet users have within it. IPL creates entitlements with a gradient in their protection: sometimes requiring consent, sometimes requiring transparency measures such as informing the user of what is done with the information, and sometimes simply imposing liability.[262]

By doing this, IPL provides entitlements that sometimes allow Internet users to exclude others—both the State and their

---

256. *See* 45 C.F.R. § 164.506(c)(2) (2016) (exchange for treatment); 45 C.F.R. § 164.506(c)(4) (exchange for healthcare operations).

257. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1189–92 (2015).

258. *See* Ignacio N. Cofone, *A Healthy Amount of Privacy: Quantifying Privacy Concerns in Medicine*, 65 CLEV. ST. L. REV. 1, 3, 23 (2016); Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN. ST. L. REV. 777, 788 (2016).

259. *See* Ohm, *supra* note 257, at 1190.

260. *See id.* at 1140.

261. 18 U.S.C. §§ 2701–12 (2012). *See* Theodore Rostow, Note, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REG. (forthcoming 2017).

262. *Cf. generally* Calabresi & Melamed, *supra* note 18.

peers—from accessing and using their personal information, and sometimes protects them with other levels of magnitude. IPL does this, for example, by defining the appropriate channel for information flow even without agency on the side of the user, or by compensating them in case of harm.[263] An example of this trend of protection without exclusion is the establishment of data breach notification requirements at state level—and the attempt to do so at federal level.[264] Protections of this kind give Internet users rights over their personal information sometimes through differing degrees of exclusion and sometimes through other strategies.[265]

VI. CONCLUSION

The way we treat our personal information and the limits of our privacy changes with new technologies. The Internet, the biggest agent in this change, has become a zero marginal cost distribution channel for both voluntary and involuntary exchanges. It turned from a system of information storage by some and information retrieval by others to a system where everyone creates and retrieves content. As a result, incentives to produce content must be given not solely to companies but also to users. While personal information can be given costlessly to others, it is still costly to produce. This implies the existence of spillovers that potentially lead to a deficit problem with too little

---

263. *Id.* The central rights of European DPL, such as the right to know, the right to access, the right to object, the right to refuse, and the right to be forgotten, are examples of this idea. *See* Council Directive 95/46, art. 12, 14, 1995 O.J. (L 281) 31, 42–43 (EC) (defining the rights to access and object, respectively). The main EU duties of data controllers, such as the duty to provide security in processing, the duty to maintain confidentiality of communications, the duty to specify a limited and justified purpose for collecting or processing, and the requirement of consent for secondary processing of data, operate in the same way, and also give differing levels of exclusion. *See* Council Directive 2002/58, art. 4, 5, 2002 O.J. (L 201) 37, 43–44 (EC) (describing the "security" and "confidentiality" requirements, respectively, of data processors).

264. H.R. 1704, 114th Cong. (2015).

265. In the EU, the right to know and the right to access, for example, merely reduce information asymmetries, and they do not limit the data controller in her use of the information. The rights to object and to refuse, on the other hand, give users a higher level of exclusion: the possibility to stop data collection if there is no legitimate basis of processing. *See* Samuelson, *supra* note 133 (explaining that "[b]ecause individuals generally have a legal right to exclude other people from access to their private data, they may have a sense that they have a property right in the data as well as a legal right to restrict access to it").

information being produced—a dynamic much like the one addressed through copyright.

Personal information in the Internet can be characterized as: (i) a public good, (ii) a good that can be disseminated at a low cost, and (iii) a good that is not yet available. Because this good is produced as a by-product of a consumption activity, IPL is not the only tool that can foster its production; the market can induce some level of information even in the absence of privacy, although this level is likely suboptimal. Given the public good characteristics of information, an optimal level of production can only be achieved through a regime that internalizes information's positive spillovers to its producers. The allocation of entitlements defines that degree of internalization and IPL, in such a way, can establish production incentives and foster the generation of information. Some level of privacy creates incentives to disclose personal data and generate information, thereby reducing the deficit problem.

Hence, the interdependence between privacy and access to information in the context of new technologies is not negative: privacy and information are often not at a tradeoff. Zero privacy would lead to a persisting deficit problem and a low level of information production (dynamic effect of IPL), while absolute privacy would lead to a high level of information production but no information flow (static effect of IPL). That information privacy is not opposed to creating an information society is good news.

As a result, some level of privacy can induce more disclosure, meaning more generation of information. More concretely, the relation between privacy and the amount of information available forms a hill-shaped concave function, where either no privacy at all or maximum privacy reduce the amount of information available. A right to privacy within information technology is desirable if one wishes to increase information disclosure.

This leads to the question of how to best protect these entitlements. Any of the three canonical entitlement protections by themselves (liability rules, property rules, or inalienability rules) would undermine the utility of IPL. For liability rules, the problem arises from a causal uncertainty problem that is unresolvable with the traditional means used elsewhere. For property rules, principal-agent relations are the problem. For inalienability rules, the benefits of information production would

be offset by a reduction in information flow—at this high level of protection, privacy and information would have a negative relationship, as illustrated in Figure 1.[266]

Recognizing this relationship between privacy and information flow, an approach that combines the first two rules would maximize both privacy and access to information for Internet users. This provides a direction for IPL: an optimal privacy-protection system should present a mixed protection, which provides varying scopes of exclusion, higher than liability rule protection and lower than property rule protection. Moreover, given the differences between IPL and copyright, the level of exclusion or propertization for IPL should be lower than for copyright law. IPL has significant similarities with the protection for copyrighted works and, where it differs, the explanation lies in the different incentive structures that arise due to the characteristics of information under IPL.

Whether to implement exclusion, and what level of exclusion is desirable, will depend on the type of information. From an economic perspective, IPL should take into account (i) who incurred costs to generate the information, (ii) the social benefits that can derive from the use of such information, and (iii) the size of the expected externalities of its use for Internet users given the type of information involved.

In sum, these considerations lead to three conclusions. First, privacy and access to information are not countervailing rights; the social costs of lacking privacy include the underproduction of information. Second, an optimal level of exclusion to incentivize the production of personal information depends on context and is generally lower than that provided by property rules, and lower than that of copyright, but higher than that of liability rules, and it will depend on the type of data in question. Third, the optimal level of protection depends on the type of information involved. An IPL that follows the type of information can address this concern and would be more efficient for this purpose than either an omnibus or an industry-specific approach.

By focusing on IPL as a mechanism to promote the generation of information, moreover, the approach introduced with this article closes two gaps in the privacy literature. First, the question of why privacy is relevant is answered by seeing

266. *See supra* Part III.

that the placement of its entitlement matters for production and that transaction costs are not low. Second, the question of how property elements over personal information can be justified in the face of the alleged mismatch between the reasons to protect personal information and to protect intellectual property[267] is addressed by showing that both copyright and IPL foster the generation of information.

267. Samuelson, *supra* note 133.