New Directions in Privacy: Disclosure, Unfairness and Externalities

Privacy Law Scholars Conference

June 2010

Mark MacCarthy

Georgetown University

"...the solution to regulating information flow is not to radically curtail the collection of information, but to regulate uses."[1]

I. INTRODUCTION

Several developments in 2009 and 2010 underscored a return of public concerns about collection of personal information by businesses and its possible misuse. In 2009 and 2010, the Federal Trade Commission conducted a series of roundtable workshops on information privacy and is preparing a report on the issue.[2] In early 2010, the Obama Administration announced that it was conducted an extensive interagency review of commercial privacy that has resulting in a notice of inquiry regarding information practices.[3] In May 2010, Representative Rick Boucher (D-VA), Chairman of the U.S. House of Representatives Subcommittee on Communications, Technology, and the Internet, and Cliff Stearns, Ranking Member of the Subcommittee, released draft legislation aimed at regulation the privacy practices of online behavioral advertisers.[4]

The concern was international. In 2010, on the 30th anniversary of the 1980 privacy guidelines, the Organization for Economic Cooperation and Development held a series of workshops and conferences on developments in privacy and scheduled a review of the guidelines for 2011.[5] Also in 2010, the European Commission announced an examination of its Data

[1] Daniel Solove, The Digital Person, New York University Press, 2004, pp. 91-92
[2] Federal Trade Commission, Exploring Privacy: A Roundtable Series, http://www.ftc.gov/bcp/workshops/privacyroundtables/
[3] Department of Commerce, Notice of Inquiry, Information Privacy and Innovation in the Internet Economy, 75 FR 21226, April 23, 2010 (Commerce Privacy NOI) available at http://www.gpo.gov/fdsys/pkg/FR-2010-04-23/pdf/2010-9450.pdf
[4] U.S. Congressman Rick Boucher, Press Release, Boucher, Stearns Release Discussion Draft of Privacy Legislation, May 4, 2010(Boucher Draft) available at http://www.boucher.house.gov/index.php?option=com_content&view=article&id=1957:boucher-stearns-release-discussion-draft-of-privacy-legislation-may-4-2010&catid=33:2010-press-releases&Itemid=41. The initial reaction was not favorable from either privacy advocates or industry representatives. See "Proposed Privacy Legislation Wins Few Fans," Wall Street Journal, May 4, 2010 available at http://blogs.wsj.com/digits/2010/05/04/proposed-privacy-legislation-wins-few-fans/tab/print/
[5] OECD, The 30th Anniversary of the OECD Privacy Guidelines, http://www.oecd.org/document/35/0,3343,en_2649_34255_44488739_1_1_1_1,00.html.

Protection Directive to see if parts of it need to be upgraded in light of new economic and technological developments.[6]

In 2009 and 2010, privacy advocates have became more active, releasing complaints regarding the privacy practices of some of the biggest companies providing services on the Internet. When Facebook announced changes in its privacy policy in December 2009, a group of consumer and privacy groups quickly filed a complaint at the Federal Trade Commission, alleging that the new changes lessened privacy.[7] In April 2010, a group of U.S. Senators wrote to the FTC repeating some of these concerns about Facebook's policies and asking the agency o establish new rules protecting users' privacy by requiring Facebook and other social networks to obtain affirmative opt-in consent before sharing information.[8] In May 2010, EPIC and other privacy groups filed an additional complaint with the Federal Trade Commission regarding Facebook's information sharing policies.[9]

In April 2010, Privacy International brought complaints of privacy violations by Google to the attention of privacy commissioners in 16 countries, alleging that its popular email service failed to obtain proper consent from its users and had engaged in illegal searches of email traffic.[10] At the same time, the Privacy Commissioner of Canada, joined by 10 other privacy Commissioners, wrote to Eric Schmidt, the CEO of Google, Inc. raising concerns about the disclosure of personal information when Google introduced its new social networking service, Buzz.[11]

But what is the best way to protect privacy? As the regulatory and legislative debate over privacy policy re-ignited in 2010, many of the concerns raised by privacy advocates and political leaders focused on the lack of control by data subjects over the collection and use of their personal information, and propose policies to increase individual control over the collection and use of information. [12]

---

[6] European Commission, Freedom, Security, and Justice, Data Protection, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

[7] EPIC et al, Complaint in the Matter of Facebook, December 17, 2009 available at http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf

[8] Letter to Marc Zuckerberg from Senators Schumer and others, Aril 27, 2010 (asserting that personal information of Facebook users "should remain private *unless* a user decides that he/she would like to make a connection and share this information with a community.") available at http://schumer.senate.gov/new_website/record.cfm?id=324226

[9] EPIC et al, Complaint in the Matter of Facebook , May 5, 2010 available at http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

[10] Privacy International, PI files complaints in sixteen countries against Google mail, April 4, 2010 available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-183142

[11] Jennifer Stoddard, Privacy Commissioner of Canada, Letter to Google, Inc Chief Executive Officer, April 20, 2010 available at http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm

[12] In releasing his draft privacy legislation, Representative Boucher said, "Our legislation confers privacy rights on individuals, informing them of the personal information that is collected and shared about them and giving them greater control over the collection, use and sharing of that information." See Boucher press release

In the United States this "informed consent" model had been the standard framework for privacy regulation for well over a decade.[13] The informed consent approach had endured because it was based on two compelling ideas: that privacy has to do with the ability of data subjects to control of information about them and the idea that people have very different privacy preferences.[14] In principle, informed consent allowed data subjects to control information according to their own preferences.

The informed consent model has been widely criticized as an expensive failure.[15] The Internet privacy policies and the federally mandated financial privacy notices are often cited as examples of the failure of this approach. They are largely unread, not very informative, and too broadly written. And they would be astonishingly costly to read. In 2009, researchers at Carnegie Mellon estimated that the cost to the economy of the time spent reading Internet privacy notices would be $781 billion per year.[16]

But the problems are more fundamental. Restrictions on disclosure are impractical in a digital world where information collection is ubiquitous, where apparently anonymous or de-identified information can be associated with a specific person and where data analytics on large or linked data bases can allow extraordinary and unpredictable inferences.[17] It is no longer reasonable to expect a typical Internet user to understand what information is collected about him or her online, what can be inferred from that information, and what can be done with the profiles and analytics based on that information. In this context, to rely on informed consent to prevent information harms would be similar to letting people decide for themselves what level of exposure to toxic substances they would accept in the workshop or the environment.

Of particular concern are negative privacy externalities, where one person's decision to share information can adversely affect others who choose to remain silent. This notion of a negative privacy externality does not rely on intangible non-quantifiable feelings of privacy

---

[13] It is the basic structure for the Children's Online Privacy Protection 23 Act of 1998 (15 U.S.C. 6501 et seq.), the FTC's privacy principles (see Federal Trade Commission, Fair Information Practice Principles, available at http://www.ftc.gov/reports/privacy3/fairinfo.shtm) and the financial privacy provisions in Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq. I call it the informed consent model rather than the notice and choice (or notice and consent) model because it directly states its enormous normative appeal. People can be said to express their approval of a social practice if they fully understand it and willingly engage in it. A social practice has strong normative appeal when individuals have so consented to it.

[14] In their modern incarnation, both ideas derive from Alan Westin.

[15] See Fred H. Cate, The Failure of Fair Information Practice Principles, in Consumer Protection In The Age Of The Information Economy (Jane K. Winn ed., 2006) ("Failure of Fair Information Practice Principles") http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972 and Daniel Weitzner et al, "Information Accountability," Computer Science and Artificial Intelligence Laboratory Technical Report, June 2007 (Weitzner) available at http://dspace.mit.edu/bitstream/handle/1721.1/37600/MIT-CSAIL-TR-2007-034.pdf?sequence=2

[16] Aleecia McDonald and Laurie Cranor, "The Cost of Reading Privacy Policies," I/S: A Journal of Law and Policy for the Information Society, 2008 Privacy Year in Review issue. http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[17] The Department of Commerce summed up these criticisms as follows: "…the customary notice and choice approach to consumer protection may be outdated, especially in the context of information-intensive, Web-based services…online interactions and web-based information linkages have become so complicated that it is increasingly difficult to provide consumers truly meaningful notice and choice. Commerce Privacy NOI p. 21229 available at http://www.gpo.gov/fdsys/pkg/FR-2010-04-23/pdf/2010-9450.pdf

violations, and it allows the conceptualization of privacy as inherently social. Under this conception, privacy concerns can express reservations about an indefinitely large class of possible economic harms that the mere refusal to disclose would not avoid. Even when individuals have the ability to refuse data collection requests, if enough other people go along with the information collection and use scheme, the economic damage is done.

Despite its intuitive appeal informed consent does not by itself render an information practice legitimate. The informed consent approach also fails to accommodate circumstances where consent is not required in order for a practice to be legitimate. Sometimes, a beneficial information practice can be rendered uneconomic, substantially less attractive or pointless if participation is less than complete. In these cases, allowing non-participation through informed consent would be to forego the benefits of a desirable information practice. Other ways of protecting people from harm have to be used. The Fair Credit Report Act, for example, regulates the use of information for eligibility decisions such as employment, insurance and credit, but it does not allow individuals to opt-out of this data collection and use.[18] Instead, it restricts the use of the data, imposes specific obligations on data collectors and users and grants access and other rights to data subjects to enable them to protect themselves.

The informed consent model seemed to be falling out of favor with U.S. government regulators as the Administration and the FTC began their review of privacy policy in 2009. However, perhaps because it is not clear what can replace it, the informed consent model has resurfaced as the default privacy framework.[19]

A policy framework containing something in addition to disclosure is needed. Two examples illustrate this extra dimension. Information security policy does not rely on informed consent. If data controllers do not keep information secure, the Federal Trade Commission treats this as an unfair practice and requires reasonable security procedures. Financial regulation no longer relies exclusively on disclosure. Some lending and credit card practices are simply prohibited as unfair. No amount of disclosure can render them legitimate. The focus in these cases is not on consent, but on whether a practice imposes substantial injury on consumers that they cannot reasonably avoid and which has no compensating benefits.

---

[18] 15 U.S.C. 1681

[19] See introductory remarks of Federal Trade Commission Chairman Jon Leibowitz: "We do feel that the approaches we've tried so far – both the notice and choice regime, and later the harm-based approach – haven't worked quite as well as we would like. But it could be that this issue is a lot like Churchill's view of democracy: "it has been said that democracy is the worst form of government except all those other forms that have been tried from time to time." FTC Privacy Roundtable, December 7, 2009, available at http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf. See also Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. Times, Aug. 4, 2009, *available at* http://www.nytimes.com/2009/08/05/business/media/05ftc.html (quoting David Vladek, the head of the FTC's Bureau of Consumer Protection as saying "The frameworks that we've been using historically for privacy are no longer sufficient."). Despite this concern over the notice and choice framework, however, the draft Boucher-Stearns privacy bill reflected the older notice and choice approach.

A similar unfairness framework for privacy needs to supplement the informed consent model. One way to structure an unfairness framework is by dividing the collection and use of information into three categories. Harmful or impermissible collection and use of information is so harmful that even with data subject consent it should not be permitted. Public benefit use of information is so important it should be allowed even without data subject consent. In between lies the realm of consent, where information can be collected and used subject to an opt-in or opt-out regime. An opt-in regime makes sense for the information uses that are closer to the impermissible uses and opt-out would be adopted for the information uses closer to the public benefit use.

The standard for determining unfairness in this privacy regulation model is the standard adopted under the FTC Act: an information practice would be unfair when it imposes substantial injury on consumers that is not easily avoidable and which does not have compensating benefits.[20]

The unfairness framework does not eliminate the use of informed consent. But it thinks of consent as a mechanism to achieve other goals, rather than an end in itself. The Do Not Call rule, for example, rested on the assessment that unsolicited telemarketing calls posed the risk of intrusion and inconvenience. Consumers needed a way to protect themselves from that harm. It did not ban the practice, and did not restrict access to telephone numbers. Instead, it used the mechanism of a "Do Not Call" list maintained by the Federal Trade Commission to allow consumers an easy and convenient way to opt out.[21]

In effect, the FTC in adopting its do not call list was making a judgment about the expected social utility of telemarketing calls, and was using a choice framework to put that judgment into effect. If the information practice in question was a public benefit uses such as medical research, the FTC would not have gone to the trouble of creating an easy and convenient way to opt out of it.

Discussions of opt-in versus opt-out are essentially discussions of the default for an information practice. This is so because very few people modify the underlying default choice. An opt-in requirement for choice is a "nudge" in the direction of discouraging the underlying information practice. An opt-out requirement is a nudge in the other direction. No reliable judgment about which direction public policy should lean can be made in the abstract. It depends on context and an assessment of an information practice in that context.[22]

An attempt can be made to avoid a direct evaluation of the value of an information practice by talking instead about the type of information involved. If information is "sensitive"

---

[20] 15 U.S.C. 45(n)

[21] Telemarketing Sales Rule - 16 CFR Part 310 available at http://www.ftc.gov/bcp/rulemaking/tsr/index.shtml. This rule was adopted under explicit authority granted by Congress rather than under the FTC's general unfairness authority, but it illustrates one way in which consent can be incorporated into an unfairness framework.

[22] See Richard Thaler and Cass Sunstein, Nudge, Penguin Books, 2009 for further discussion of the use of policy defaults.

then consumers have to be given a greater degree of control. But this inevitably creates overly broad rules such as a rule requiring affirmative express for all uses of financial information. To remedy this defect of over breadth, a series of exceptions from the rule are crafted, such as for operational or fraud uses.[23] But a list of exceptions cannot be flexible enough to cover the possible information uses that might provide significant benefits. The result is that as a practical matter the opt-in rule for information uses involving financial information or for "sensitive" information generally acts as a barrier to innovation in that area.

To move forward with the unfairness framework requires greater understanding of how information is used to provide goods and services to people. The first step would be an inventory of current and innovative information uses in particular contexts, and an ongoing survey of developments. The second step is a process whereby these information uses can be assessed and the appropriate regulatory structure, if any, put in place. In the unfairness framework, choice is one, but only one tool to be used to construct an adequate system that will encourage beneficial innovative uses and protect data subjects.

The contrast between the models of privacy regulation can be seen by examining the privacy issues raised by online behavioral advertising and social networks. The informed consent model focuses on the nature of disclosure and the kind of choice involved. It would encourage or require more flexible, transparent and granular notice and choice – going well beyond the unread, uninformative privacy notices that have characterized the older privacy regimes. It would impose a default allowing use in some case, and blocking it in others.

In contrast, the unfairness models asks what the information collected is used for and what benefits and harms can result from that use. For example, some estimate that targeted ads can increase revenue for the websites that use them by 50% compared to generic ads. If this is so, then online behavioral advertising creates substantial advantages for the continued free delivery of online content, including for online outposts of newspapers that face an economic crisis. A choice regime that unduly restricts online behavioral advertising might be very damaging to the continued deployment of diverse online content.

On the other hand, the biggest dangers associated with online behavioral advertising might come from the possible secondary use of the profiles and analytics constructed to enable targeted advertising. What restrictions should be placed on these secondary uses? A notice and choice regime that imposes a default of no use has not avoided making an assessment of these uses. Instead, through this policy "nudge" it has effectively ruled out such additional uses.

An unfairness regime would look at the possible uses and try to assess which ones might be damaging. For example, the use of these profiles for eligibility decisions such as employment, insurance or credit might not be beneficial. If it were generally known that online behavioral profiles could be used for these purposes, this might dramatically curtail the

[23] This is the approach taken by the draft Boucher bill and suggested by the FTC draft principles.

widespread, open and robust use of the Internet itself. Policymakers might want to weigh this risk against any likely benefit in improved predictions on eligibility decisions, and might ultimately determine that, on balance, this use was so harmful it should not be allowed. However, if it makes sense to allow these uses, then it makes sense to make sure that they fall under the right regulatory regime, such as the rules and protections provided by the FCRA.

The same point that policy makers have to assess secondary information uses applies to privacy issues involving social networks. Profiles are already being constructed by companies based upon information derived from social networks and apparently being used to guide decisions involving the marketing and granting of credit. More granular and flexible privacy notice and choice regimes have been proposed as the way to deal with privacy in social networks. But the unfairness model suggests a different approach. The assessment of these uses of social networking information should not remain at the level of the individual and the firm, as would be called for under the informed consent model. Under the unfairness model, it would require the active and direct involvement of public policymakers in the assessment of the secondary uses of information gathered by social networks.

Part I of this paper describes the limitations on the informed consent model, suggesting that informed consent is neither necessary nor sufficient for a legitimate information practice. Part II explores the idea of negative privacy externalities, illustrating several ways in which data can be leaky. It also discusses the ways in which the indirect disclosure of information can harm individuals through invidious discrimination, inefficient product variety restrictions on access, and price discrimination. Part III outlines the unfairness model, explores the three-part test for unfairness under the Federal Trade Commission Act, and compares to model to similar privacy frameworks that have been proposed as additions to (or replacements for) the informed consent model. Part IV explores how to apply the unfairness framework to some current privacy issues involving online behavioral advertising and social networks.

II. THE LIMITATIONS ON INFORMED CONSENT

A. The Informed Consent Model

Privacy rules can be thought of as procedural or substantive. The procedural rules tell data collectors and users how they should go about obtaining information. Essentially, they specify what kind of notice and what kind of choice they have to provide. The substantive rules put some limits or requirements on what data collectors and users can do with the information. Rules that require data minimization or deletion or that prohibit redlining or discrimination or sharing or secondary use are substantive.

The informed consent model reduces privacy policy to procedural rules. It can be summed up in two propositions: informed consent is necessary to obtain legitimacy and it is

sufficient. With informed consent, any information collection and use practice is legitimate. Without it, no information collection and use practice is legitimate.

The original fair information practices developed by HEW express this idea of informed consent.[24] Several versions of subsequent fair information practices contain this notion as well, including the1980 OECD guidelines[25] and the 1995 European Union's data protection directive.[26] The FTC summed up the notice and choice elements of informed consent: "without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information." This notice should tell consumers "what will happen to the personal information they are asked to divulge."[27]

The informed consent model is sometimes thought of as a U.S. variant of the more general fair information practices. But fair information practice principles include more than just notice and consent.[28] The OECD guidelines for example include the principles on collection limitation, data quality, purpose specification, use limitation, security safeguards, openness and individual participation.[29] Whatever is true of the U.S. variant, the more general fair information practices principles go well beyond notice and choice. But even the restricted set of U.S. fair information practices includes security and access as well as notice and consent.[30] Looked at this way, privacy policy of both the European and U.S. variety seem to contain much more than just informed consent.

It is appropriate to focus on the role of individual consent as the heart of the current approach to privacy for several reasons. First, the other fair information practice principles do not relate to whether the collection and use of information itself is legitimate. The security safeguard principle, for example, is designed to prevent unauthorized access to information. Its goal is to protect data subjects from harms such as fraud and identity theft. The access and correction and the data quality principles are aimed at providing individuals with the opportunity to correct the record and to block the use of inaccurate or out of date information. Second, the

---

[24] Three of the five HEW principles focus on knowledge of data collection and use: There must be no personal data record keeping systems whose very existence is secret. There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. U.S. Department of Health, Education and Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computer, and the Rights of Citizens (1973) at viii. Available at http://aspe.hhs.gov/datacncl/1977privacy/toc.htm.

[25] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Oct. 1, 1980. The collection limitation, use limitation and openness principles all seem to require consent. (OECD Privacy Guidelines) available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[26] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Eur. O.J. 95/L281). (European Data Protection Directive) The purpose limitation and transparency principles relate to knowledge and consent.

[27] Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[28] See Bob Gelman, Fair Information Practices: A Basic History Version 1.8 April 12, 2010, (noting at p. 8 that " *Notice and choice* is sometimes presented as an implementation of FIPs, but it typically falls well short of FIPs standards.") available at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

[29] OECD Privacy Guidelines

[30] Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace, (May 2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

other principles such as openness, individual participation, collection limitation and so on are aimed to establish, maintain and reinforce the ability of individuals to make informed judgments about the collection and use of data. The justification of limits on secondary use, for example, is not that these uses are improper but that people cannot exercise choice about secondary uses unless they are first presented with a description of the possible uses and asked to accept them.

Informed consent then has a good claim to be the heart of privacy policy as currently conceived in both the European and U.S. policy frameworks. It has endured as the touchstone of privacy policy because it is based on two compelling ideas: that privacy has to do with the control of information about data subjects and the idea that people have different privacy preferences. If an institution has access to detailed profiles about data subjects, this gives it the power to make decisions that might adversely affect the interests of those data subjects. Privacy has something to do with restoring some control to the data subjects in this situation.[31] But people differ in the extent to which they care about privacy. Some do not want anyone else to know what they are up to; some are happy to let the world know, and most people think it depends.[32] Informed consent marries the two ideas: if people control the information flow, they can protect information according to their own preferences.

Consent can vary along a continuum, depending on the extent to which the terms and conditions on information collection and use are modifiable by the data subject. At the one end of the continuum, the data collector presents a take-it-or-leave-it set of information collection and use conditions. The data collector discloses what information it wants to collect from a user as a condition of providing a service and then specifies what it intends to do with the data. The consent is obtained when the user provides the information and uses the service. If people do not want this collection and use of information, they are free to not do business with the company.

Under this take-or-leave-it regime, the informed consent model focuses on the quality of the disclosure and the ease with which people can gain access it, and the language it is written in. If a privacy policy is insufficiently revealing, the company might be subject to remedial action to reveal more. If it is misleading or deceptive, the company might be forced to revise the disclosure to make it more accurate. If the disclosure is too hard to find, or not available at the time that a potential customer must make a decision to use the service, then changes can be required to make the disclosure conspicuous and timely.[33] But if a company announces at the time of the service offering, clearly and conspicuously what it intends to do with information and

[31] The modern starting point for this notion of information privacy as control is Alan F. Westin, Privacy and Freedom (New York: Atheneum, 1967) where he defines information privacy (p. 7) as " the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

[32] Based on a series of surveys, Alan Westin developed a privacy index describing people as (1) High and Fundamentalist, (2) Medium and Pragmatist, or (3) Low and Unconcerned. See Ponnurangam Kumaraguru and Lorrie Faith Cranor, Privacy Indexes: A Survey of Westin's Studies CMU-ISRI-5-138 December 2005 available at http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf

[33] The Federal Trade Commission uses its authority to prevent deceptive practices to set terms and conditions for notice and choice. For a recent example, see Federal Trade Commission, Complaint In The Matter Of Sears, September 9, 2009 available at http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf

does that and nothing else with the information and the data subject agrees to this by continuing to do business with the company, there is no further cause for complaint.

At the other end of the continuum, all terms of information collection and use are negotiable except for the minimum needed to provide the service. The company can set a default, and the user can change that. If the default is set at zero collection of information, the user must then change that, or opt-in for data collection. If the default is set at maximal collection of information, then the user must opt-out of information collection if he objects. Varying mixtures of opt-in and opt-out are possible. The key elements from a public policy perspective are the quality, timeliness and accessibility of the disclosures and the nature of the choice.

Informed consent involves three elements: the collection itself, the purpose for which the data is collected and any secondary use of the data. The informed consent model allows variants according to whether disclosures of the purpose of information use must be specific or whether broad descriptions of possible uses are acceptable. Under some versions, it would be acceptable to ask for general consent to all future uses. Most versions, however, contemplate specific disclosures for the immediate purpose of the data collection. If a further specific use is later contemplated, then further disclosure and additional consent is required.[34]

So that is the sufficiency prong of the informed consent model. Informed consent makes an information practice legitimate. The other part of the informed consent model is that hidden information gathering and use that the data subject has not agreed to is illegitimate. There has to be informed consent. Otherwise the practice, no matter how benign or beneficial, is unacceptable. This necessity prong of the informed consent model expresses the idea that secret gathering of data profiles and their use for unannounced purposes without the knowledge and consent of the data subjects is the essence of information privacy harm.

Public policy under an informed consent model examines a variety of disclosure questions. But the basic questions are only two: Is the disclosure adequate? Is the type of choice provided (take-it-or-leave-it, opt-in, opt-out) appropriate for the type of information collected and the uses to which it is put? Once satisfied about the quality of disclosure and the conditions of choice, privacy policy is done.

The informed consent model is entirely focused on the individual. No policymaker looks at information use and decides whether it is good or bad. Knowledge of what is done with information collected has to be provided to individuals, but not to government officials. Evaluation of information uses is done entirely by individuals. With enough disclosure about information uses, and the right sort of mechanisms for consent, people are individually empowered to decide which uses of information are worth it to them. The sum total of these

[34] Article 6 of The European Data Protection Directive, for example, imposes these restrictions. See the summary discussion in Peter Swire and Robert Litan, None of Your Business, Brookings, 1998, pp. 28-31.

individual decisions determines the nature and size of information collection and use in society. Policymakers focus on making sure that the conditions are right for individual-level choice and do not themselves engage in substantive evaluation of information uses.

B. Criticisms

One line of criticism of the informed consent model is that it is expensive and impractical. The financial privacy notices that were required by federal legislation following the passage of the Gramm-Leach-Bliley privacy requirements illustrate the weakness of the disclosure approach. Billions of dollars were spent designing, testing, and mailing (every year) privacy notices that almost no one reads and that are virtually incomprehensible if read.[35] No one's privacy is furthered by these empty requirements on formal notification. Privacy policies on the Internet are equally unread. And it's a good thing. These policies too are virtually incomprehensible and astonishingly costly to read. Researchers at Carnegie Mellon concluded that if all U.S. consumers read all the privacy policies for all the web sites they visited just once a year, the total amount of time spent on just reading the policies would be 53.8 billion hours per year and the cost to the economy of the time spent doing this would be $781 billion per year.[36]

Additional objections to the informed consent model based on the practicalities of informing people and obtaining their consent are well taken.[37] An additional objection to be explored in greater detail below arises from the development and growth of data collection, aggregation and analytics over the last decade. It no longer seems reasonable to expect people to fully understand how information can flow, how it can be analyzed and how information about them can be used.[38] Fully informed consent is no longer a reasonable goal.

It is worth spelling out these limitations in two parts. Informed consent is neither sufficient nor necessary to make an information practice legitimate.

C. Informed Consent Is Not Necessary

The informed consent approach fails to accommodate circumstances where consent is not required in order for an information collection and use practice to be legitimate. This is not a matter of it being too expensive to tell people about a practice and obtain their consent. In some

---

[35] Fred H. Cate, The Failure of Fair Information Practice Principles, in Consumer Protection In The Age Of The 'Information Economy' (Jane K. Winn ed., 2006) ("Failure of Fair Information Practice Principles") http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972 (noting at p. 365 that financial privacy notices cost an estimated $2-5 billion)

[36] Aleecia McDonald and Laurie Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, 2008 Privacy Year in Review issue. http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf. The authors do not treat their study as an argument against notice and choice, but as an indication that privacy has to be made easier to understand.

[37] Cate, Failure of Fair Information Practices, summarizes these limitations.

[38] See Weitzner, p. 1. Lundblad and Masiello make a similar point: "According to some, online interactions and web-based information linkages have become so complicated that it is increasingly difficult to provide consumers truly meaningful notice and choice." N Lundblad and B Masiello, "Opt-in Dystopias", (2010) 7:1 *SCRIPTed* 155, http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp

cases, people should not have the ability to reject information collection and use because this will block uses of information that have important public benefits that we want to allow. It is useful to review just a few examples of this.

The Fair Credit Reporting Act[39] was designed to regulate the activities of data collectors and to protect the data subjects. It involved trade offs between the need for this information to be collected and used and the interests of data subjects. One significant trade off was the restriction of the ability of individuals to block the use of information about them in credit reporting files. Files can be furnished only for permissible purposes which include employment screening, insurance underwriting, credit granting and child support payments.[40] The file can also be released with the written consent of the data subject, but such consent is not required. The permissible uses of information for eligibility decisions under Fair Credit Reporting Act includes do not allow data subjects to block these uses by withholding consent. The reason is straightforward. Credit reporting agencies gather information about individuals in order to assess their suitability for insurance, granting of credit and employment. Their files contain both positive and negative information about people and provide the ability of to assess the risk involved in making people eligible. If people who were bad risks were able to withhold information from these agencies, the files would lose a large part of their value for these purposes.[41]

The Drivers Privacy Protection Act was passed to prevent states from selling drivers license records or otherwise releasing to the public the information collected as part of the licensing procedure. It was passed in response to public concern about these practices, someone of which created a threat to the safety of particular individuals. The DPPI allows only certain permissible uses of drivers' license records and does not allow the data subject to stop these permissible uses. These uses include legitimate government agency functions, certain legitimate business needs, use in connection with court proceedings, certain research and insurance activities, and for any other legitimate State use if it relates to motor vehicle or public safety. DPPI allows release of the information if the state has obtained express consent from the individual, but it does not require this consent for other permissible uses.[42]

Title V of the GLBA of 1999 provides for various privacy protections for consumers of financial service institutions. In particular, it provides for notice and the opportunity to opt-out of various information sharing and use practices. For instance, it allows consumers to opt-out of

[39] 15 U.S.C. § 1681 et seq. available at http://www.ftc.gov/os/statutes/031224fcra.pdf.
[40] 15 U.S.C. § 1681b
[41] J. Howard Beales, III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information 75 U. Chi. L. Rev. 109 2008 ("Beales and Muris"), pp. 116-117
[42] 8 U.S.C. § 2721, available at http://www4.law.cornell.edu/uscode/18/2721.html. See further information and background at Electronic Privacy Information Center, The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record, available at http://epic.org/privacy/drivers/

information sharing with unaffiliated third parties.[43] There are a number of circumstances when the law does not allow the consumer to opt out of information sharing, including:

- to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein
- to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability
- for required institutional risk control, or for resolving customer disputes or inquiries
- to persons holding a legal or beneficial interest relating to the consumer;
- to persons acting in a fiduciary or representative capacity on behalf of the consumer[44]

The idea behind these exceptions is that the sharing of information with third parties for these purposes has benefits to the consumer and to society that outweigh the interest in allowing the consumer to block sharing. For instance, fraud control measures that would benefit all consumers might be adversely impacted if a large number of consumers blocked the sharing of information for data analysis to detect patterns of unauthorized use. Sharing of information is also allowed with the consent or at the direction of the consumer, but this consent is not required for the purposes listed above.[45]

These illustrative examples and others[46] indicate that consent of the opt-in or opt-out variety is not always necessary to establish the legitimacy of an information practice. Two general conditions seem to call for limitations on informed consent. One is when getting consent is so expensive that it would render a particular use uneconomic and this use is socially beneficial. Another is when the major value of the information is its completeness. In these circumstances, allowing individuals to opt out of the use would prevent the use.

Even without individual consent, rules can be established regarding the use of information that allows only those uses that are of net benefit to the public. Unlike the informed consent model of public policy decision making, however, this requires policymakers to directly confront the question of the social value of the information use.

D. Informed Consent Is Not Sufficient

The other prong of the informed consent approach is that consent can make any information practice legitimate. Even as astute an observer of privacy issues as Daniel Solove

[43] 15 USC, Subchapter I, Sec. 6802(b)(1) at http://www.ftc.gov/privacy/glbact/glbsub1.htm#6802
[44] 15 USC, Subchapter I, Sec. 6802(e)(3) at http://www.ftc.gov/privacy/glbact/glbsub1.htm#6802
[45] 15 USC, Subchapter I, Sec. 6802(e)(2) at http://www.ftc.gov/privacy/glbact/glbsub1.htm#6802
[46] Public records also are available for public use without the consent of the data subject. Court records, property records and the like are available to the public and should not be withheld at the sole discretion of the data subject. The draft Boucher privacy bill provides an exemption from notice and choice for "operational uses" which include improving a service, using analytics to improve a serve and preventing fraud and unauthorized transactions. See Boucher draft May 3, p. 4.

treats consent as curing all or most evils in information use. "The activities that affect privacy often are not inherently problematic. When a person consents to most of these activities, there is no privacy violation."[47] The issue for many defenders of the informed consent model is whether consent is really valid. Within this model, there is no room for the idea that even with valid, robust consent there could be a privacy problem.

Many critics of notice and choice also accept the idea that consent is a remedy for any information use. Beales and Muris, for example, champion an approach to privacy based on consequences not choice, but they have not broken this hold that the notice and choice model has on their thinking:

> If consumers knew that data given to one agency would be matched to data from another agency and they had a choice about whether to provide the data or allow the match, then it is very difficult to see how a privacy problem could exist. The converse, however, does not follow. That is, the absence of a privacy problem when consumers understand and have a choice about the information collection or use does not imply that a privacy problem exists whenever consumers are ignorant of the information use or lack a choice about it. [48]

Their real target is not choice itself, but the idea that choice is required for good privacy policy. As we have seen in the previous section, they are largely right about this. But they fully accept the idea that there is an "absence of a privacy problem when consumers understand and have a choice about the information collection or use." This is consistent with their general economic approach that accords priority to the fully informed preferences of individuals acting in a functioning competitive marketplace.

To see that informed consent is not sufficient for making an information practice legitimate, it is worthwhile to consider the informed consent program that governs participation in research experiments funded by the government. In this framework, Institutional Review Boards must evaluate proposed research and approve it when it meets certain conditions. One of these conditions is ascertaining that informed consent has been sought and documented. Informed consent is obtained in various ways, and requires a full explanation of the nature of the research and the risks.[49]

---

[47] Daniel Solove, "A Taxonomy of Privacy," Chapter 5 in Understanding Privacy, Harvard University Press 2008 p. 102.
[48] Beales and Muris p. 113
[49] The disclosures that must be made to potential subjects include a statement explaining the purposes of the research and the procedures to be followed, a description of any reasonably foreseeable risks to the subject, a description of any reasonably foreseeable benefits to the subject or to others, a disclosure of any appropriate alternative procedures, a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained, and a statement that participation is voluntary, that refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and that the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled. See 21 CFR Part 50 -- Protection Of Human Subjects available at http://www.research.buffalo.edu/rsp/21CFR50.htm

This framework treats informed consent as necessary, subject to various exceptions including the need for action in emergency situations. But informed consent is not by itself sufficient. Other factors must be taken into account including efforts to minimize risk, to balance risk against benefit and to ensure data confidentiality. Proposed research projects can be rejected when risk levels are too high, or where the level of risk is not justified by compensating benefits. [50] In this area, informed consent does not always render the underlying activity legitimate.

Just obtaining informed consent does not render an information practice legitimate. Some commentators come to this conclusion by reflecting on the importance of privacy as a social good, and concluded that in some circumstances "coercing privacy" would be justified. The idea is that individual choice in this area would lead in a piecemeal fashion to the erosion of privacy protections that are the foundation of the democratic regime that is the heart of our political system.[51] Others arrive there by analyzing the different ways in which privacy choices can reflect something other than considered judgment.[52] Others look at imbalances of bargaining power in the marketplace and conclude that choice in those circumstances is not reflective of consent.[53] Others reject the sufficiency prong by noting that even consensual decision making would reinforce patters of inequality that are inimical to a just society.[54]

The approach taken here is not in contradiction to these approaches. But it focuses on ways that an individual's fully informed consent about information collection and use can have harmful consequences - for others. The decision of the individual is fully rational, not a function of defective heuristic biases, or based on misleading or incomplete information.

Individual consent for information collection and use is analogous to the choice of a firm to use polluting technology in the production process when the costs of polluting are externalized to other parties. The firm is not making a mistake. It is rationally evaluating the costs to it of using productive inputs and resources. The problem is not in the quality of the thinking or the information available to the firm. The problem is that the structure of the market and the production process does not allow the firm to experience the full costs of its resource use. Other parties bear those costs. The result in the environmental case is that too much is produced using

[50] IRBs are required to ensure several conditions are satisfied before approving a project, including that risks to subjects are minimized, risks to subjects are reasonable in relation to anticipated benefits, selection of subjects is equitable, that the research plan makes adequate provision for monitoring the data collected to ensure the safety of subjects and that there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data. Obtaining informed consent is only one element in determining the acceptability of a research project. See 21 CFR Part 56 – Institutional Review Boards, available at http://www.research.buffalo.edu/rsp/21CFR56.htm#%C2%A7%2056.111%20Criteria%20for%20IRB%20approval%20of%20research.

[51] Anita Allen, "Coercing Privacy," 40 William and Mary Law Review 723 (1999)

[52] Paul Schwartz, "Privacy and Democracy in Cyberspace," 52 Vand L. Rev.1609 (1999)

[53] Daniel Solove, The Digital Person, New York University Press, 2004, p.p. 82-85.

[54] Oscar Gandy, The Panoptic Sort, Westview Press, 1993

the polluting technology. The result in the information case is that firms collect and use too much information. Individual choice is fully rational, but the result is less than socially optimal.

In the next section, I examine how information collection and use can have external effects. In the section after that I examine how these effects can be harmful. Several examples are given: invidious discrimination, group harms, inefficient product variety restricted access to goods and services and price discrimination. These examples together illustrate the point that allowing individual consent alone to determine the direction and nature of information use is not sufficient for good public policy.

III. PRIVACY EXTERNALITIES

A. Negative Privacy Externalities

People have interests that can be adversely affected by information sharing practices that they can individually avoid. Privacy harms of this kind are negative privacy externalities. They are not a separate kind of harm in addition to physical, financial and other tangible harms that can occur to individuals. Negative privacy externalities are these individual harms that are imposed upon individuals by privacy choices made by others.[55]

The first step in understanding negative privacy externalities is to understand how information about a person can leak out even when the person himself does not reveal it or it is not available in public records. Data collectors, aggregators and analysts can infer information about individuals even when these individuals do not reveal that information themselves or when it is not specifically recorded in public or private data bases to which they have access. This leakage might be described as an information externality. But by itself this information leakage is neutral. It might result in a benefit or a loss to the data subject, depending on how the information is used. The second step is to understand some of the ways in which this indirectly obtained information can be used to the detriment of the data subject. When this happens, the information externality is negative and can be described as a negative privacy externality.

When privacy is thought about as involving an externality, it is inherently social because privacy decisions made by some actors inevitably affect the economic interests of others. Even if choice could be made easily and at modest cost, it might still be the wrong way to set privacy policy, since individual level choice will result in data collection and use patterns that impose substantial tangible costs on individuals who are not directly involved in making those choices. At the individual level, one person's data disclosure choices affect others; at the social level, the data choices of a substantial number of people, perhaps a majority, might adversely affect the remainder of the population.

[55] For a good general account of externalities see Richard Cornes and Todd Sandler, The Theory of Externalities, Public Goods and Club Goods, Cambridge University Press, Second Edition, 1996, Chapters 1 and 2.

This notion of privacy externalities differs from the one typically encountered in the literature. Analysts such as Hal Varian[56] and Peter Swire[57] argue that companies collecting personal information impose a negative externality on consumers. These companies benefit from the information they collect, but do not face the costs of the violation of consumers' privacy. As in standard cases of externalities, the result is that they collect "too much" information. Their idea is that an externality exists precisely because people do not have control over the use of information. Companies are able to use the "scarce" resource of other people's information without paying them for the "privacy" costs imposed on them. This externality problem can be addressed by giving people a "property right" in their information. Then companies could use it only with their permission.[58]

The externality emphasized here is different. Here an individual's decision to share information with a data collector imposes costs on others. Individuals might have been given full "property rights" over information about themselves; the notice involved can be clear and conspicuous and timely, and the consent regime can be extremely robust – a full opt-in with no information collection or use without explicit prior informed consent. Even in those circumstances, however, there is leakage of information about individuals who do not themselves choose to reveal it. This indirectly revealed information can then be used to impose an external cost on these individuals. A system of property rights cannot correct an externality of this kind.

The use of information and analytics to construct a profile of individuals has been noted before by many commentators.[59] The concerns expressed in these works emphasize that information left by a person's "data trail" – his record of transactions, employment, property ownership, marriage, divorce, debt repayment history and so can impose costs on the individual and on society that are not outweighed by any social benefits. It has been emphasized how difficult it is to prevent the construction of these profiles by individual caution and careful information control practices.

The idea of privacy externalities adds a dimension to these concerns about profiling. Even if some individuals do not contribute information about themselves to these profiles, information provided by others can be used to make inferences about them. These inferences, indirectly revealed information, can be added to profiles and made available for further uses. It can be inferred from a wide variety of sources even when not directly revealed by a data subject.

---

[56] See Hal Varian, Economic Aspects of Personal Privacy, December 6, 1996 available at http://people.ischool.berkeley.edu/~hal/Papers/privacy

[57] Peter Swire and Robert Litan, None of Your Business, Brookings Institution, 1998, pp. 7-8

[58] There are substantial difficulties with this privacy externality analysis and the property rights solution it proposes. In essence, it is a version of informed consent, and suffers from all the difficulties of that approach that were discussed in the previous sections. Additional criticisms are in Daniel Solove, "The Limits of Market-Based Solutions, Chapter 5 in The Digital Person, New York University Press, 2004, pp.76-92

[59] Two useful surveys Daniel Solove The Digital Person, New York University Press, 2004 and Simpson Garfinkel Database Nation, O'Reilly, 2000.

This can be seen very clearly in several different circumstances. When a certain characteristic is relevant to the eligibility decision, it is impossible for a candidate to keep the relevant information secret. Scientific regularities about people also provide a way to infer the presence of one characteristic from the presence of others. If the data collector knows the independent variable in that circumstance, it can use the regularity to infer the presence of the dependent variable, even when the people involved have not revealed the presence of that characteristic and it cannot be found in public records. A special case of this type of scientific inference involves the use data analysis and data mining techniques to reveal otherwise hidden characteristics or behavior patterns of groups of people.

B. Eligibility Decisions

There are many cases involving eligibility where information disclosure by some people reveals information about other people. This can happen in several ways. When people do not reveal a particular characteristic about themselves this can be evidence that they have the characteristic. People who do not tell their insurance company about their smoking habits become smokers. College applicants who do not submit their SAT scores become applicants with low scores. Potential renters who do not list their race on the application form become members of a disfavored racial group. Job applicants who do not disclose a disability or who refuse to take medical tests that would reveal it become people with that disability.

The key element in this case is that information that could affect an eligibility decision can be expected to leak out in the context of fully informed consent for information sharing. Those who can gain from information sharing would rationally choose to reveal; those who would be adversely affected might try to avoid the adverse effect by remaining silent, but their silence is used as information against them. When the information involves sensitive categories, law sometimes restricts information sharing to prevent discrimination. Private parties can also attempt to restrict information sharing to protect the overall well being of their members.

C. Scientific Research

Normal scientific research can determine that people with one characteristic or group of characteristics have or have a high probability of having another characteristic. These can be physical, genetic, biological, demographic or social characteristics. Scientific experiments and social science surveys are designed to establish these empirical regularities.

Examples of these connections are numerous and varied. Research has established elevated risk of certain diseases in certain demographic groups.[60] This research is often used to determine that people are at risk of certain diseases, or suggest certain remedies. Social science

[60] This is the case for Tay-Sachs disease among Ashkenazy Jews and sickle-cell anemia among African Americans, for example.

research can reveal substantial information about people's motivations, beliefs, and habits and can relate characteristics to demographic data, including age, race, religion, national origin. These connections and linkages are useful for analyzing social and economic trends, planning for public investment projects such as highways and schools

The relevance for the questions of privacy externalities is that many facts about people can be inferred from other facts about them. The research that establishes these linkages is research on a subset of a population. Even if only a small minority of data subjects within a particular group are involved in the scientific research that establishes a linkage between people in that group and some characteristic, trait or behavior, all members of that group are affected. Members of other groups might be affected as well. Once the scientific linkage is established, data collectors, aggregators and analysts no longer need to obtain information about that characteristic, trait or behavior from the data subject or from public or private records of their activities. They can infer the presence of that trait from the membership in the group. They might even be able to infer the absence of that trait among members of other groups.

Statistical inferences from membership in social networks are possible as well. If researchers establish that people with obese friends tend to be obese, then once it is known that a person's social network has a high percentage of obese people in it, it can be inferred that the data subject is probably obese. In one study, for example, having obese friends made it 58% more likely that a data subject was obese.[61] And the effects spread through three degrees of separation. If a data subject has friends of friends who are obese, he was 20% more likely to be obese. Third-degree obese friends make a data subject 10% more likely to be obese. Similar influences can be made about smoking, drinking and even happiness.

Studies of smoking show that as more and more people quit smoking the remaining smokers are clustered in tight-knit groups with few connections to non-smokers. Most non-smokers also have few smoking friends. These facts provide a way for information about people's smoking habits to unravel in an employment or insurance context – even if the smoking condition is not explicitly made a condition for eligibility for a job or insurance. A company can examine a prospective employee's social network, and if they have even a minimal amount of information on the smoking behavior of the group, they can infer the prospect's smoking behavior with a reasonable degree of certainty. Without explicitly asking anyone for it, they can discover smoking behaviors.

Using the social network analysis for this purpose sounds sinister. But the same analysis can help public health officials devise an effective strategy for reducing smoking. It suggests for example that do-not-smoke warnings are ineffective and the best way to help smokers to quit is to get their friends to do it. An app has even been developed for Facebook that enables a strategy like this: it publicizes that a user of the app has stopped smoking, for how long and how much

[61] Are Your Friends Making You Fat New York Times, September 13, 2009 available at http://www.nytimes.com/2009/09/13/magazine/13contagion-t.html?_r=1&pagewanted=all

money he has saved.[62] The problem is not the inference that is made possible by scientific research but the purpose for which that inferential knowledge is used.

D. Data Mining

A particular application of social science research methods is important enough to call for special treatment. These are the analytical techniques that can reveal patterns in large and linked data sets. It is through these techniques that data subjects often reveal information about other people when they reveal information about themselves.

Commentators break down the information flow patterns into three parts. First is the data gathering phase. Second, is the data analysis phase and third is the data use phase.[63] The important phase for understanding privacy externalities is the data analysis phase, where a variety of statistical techniques are applied to aggregated and linked data sets. Two varieties of these techniques are relevant. Data analysis takes place when researchers break down the data into pre-existing subcategories, hypothesize a connection among variables in the data, test the hypothesis and either confirm or deny it. For example, researchers might create a variety of demographic-marketing niches like single urban profession, and then look for behavioral or purchasing trends within these groups.[64] Once such as pattern is found, it can be used for inferences. If a particular potential customer falls into one of these marketing niches, then it can be inferred that he shares his group's typical behavior pattern – even if no purchasing information or behavioral trends are available for that person.

Data mining refers to the discovery of patterns within the data itself without needing to formulate a hypothesis about what pattern will emerge from the examination of the data. The correlations and patterns discovered in the data are unpredictable in advance. Neither the data subject nor the data collector knows can anticipate with any certainty what patterns will emerge.[65] The newly discovered regular pattern can be used to predict information about new potential customers whose behavior has not been tracked in any data base.

The key for the purposes of understanding privacy externalities is that the regularities and patterns revealed by these techniques apply beyond the data used to generate them. Data from people who have revealed information about themselves through surveys, transactions and other

[62] See wequit at http://www.facebook.com/apps/application.php?id=337063416862&ref=search&sid=707107521.2497277038..1
[63] T.Z. Zarsky, "Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society," 56 Maine Law Review 13 (2004). (Zarsky). He uses the phrase "implementation" to describe data uses. His major theme that privacy regulation should be undertaken at the stage of usage rather than data collection or analysis is consistent with the unfairness framework developed here. An alternative typology is found in Nissenbaum, who divides the information technology landscape into the three parts of (1) tracking and monitoring, (2) data aggregation and analysis and (3) data dissemination. See Helen Nissenbaum in Privacy In Context, Stanford Law Books, 2009 (Nissenbaum), p. 11.
[64] Zarsky, p. 27
[65] Zarsky, p. 28. Neural network analysis to detect typical spending patterns in credit card transactions is an example. The card companies do not impose any pattern of spending on the card holder. Rather they let the pattern itself emerge. Marked departures from the pattern are then an indication of possible fraudulent use.

voluntary disclosures are part of the evidentiary basis for the knowledge revealed by these analytical techniques. But they apply to other people who have never disclosed that information about themselves. Both the underlying evidence and the discovered patterns are information externalities from the point of view of these people.

One hypothetical example illustrates the method. Suppose from public data records, it can be inferred that one of two people was involved in a particular transaction and that person who engaged in the particular transaction was right handed. If the left-handed person discloses this information, he or she thereby discloses that the other person engaged in the transaction.[66]

These indirect disclosures are usually probabilistic rather than certain. Most personalization functions at online outlets such as movie book or music websites involve privacy externalities. If an online store knows that two people share most of their book purchases in common and know that, in addition, one person likes murder mysteries by Agatha Christie, it can make the inference with a reasonable degree of certainty that the other person will like Agatha Christie novels. The online bookstore's Agatha Christie recommendations are based on this probabilistic inference.[67]

Information revealed in the context of eligibility decisions, through standard scientific research or through data mining will provide data collectors and users with increasing amounts of information about data subjects that has been revealed by the disclosure decisions of others. The dramatically expanded use of data mining techniques seems likely to be an especially rich source of indirectly revealed information. This increasingly large pool of indirectly revealed information can then be used for a variety of purposes.

Some of these purposes are clearly beneficial on balance. Most people, for example, like the convenience of recommendations based on other people's disclosure of their shopping patterns. Those who do not find them useful are free to ignore them. If there is any harm from these recommendations, it is easily avoidable and is more than balanced by the extra information that make shopping more convenient for other people.

But some of these uses made of indirectly revealed information will be harmful to data subjects and on balance they might be harmful to society. This leads to the second part of the discussion of negative privacy externalities – the harmful use of indirectly revealed information.

E. Harms

[66] Thanks to Ed Felton for this "teaching" example.

[67] There is nothing that restricts these inferences to data mining in large and linked data sets of information about people's online behavior. It is possible whenever information about one person can be linked through common patterns or structures to information about other people. For instance, genetic information about one individual in a family can be inferred from if the genetic structure of a large enough set of relatives is known.

In this section, I examine various harms that can occur from the indirect disclosure of information. These are invidious discrimination, group injury, inefficient product variety, restricted access to products and services, and price discrimination.

1. Invidious Discrimination

Information can be used to deny access to employment, insurance, credit and a variety of other services and benefits based upon objectionable criteria. For this reason, legal limitations sometimes prevent people from collecting information thought to be an inappropriate basis for decision. These protected categories include races, sex, age, national origin. In an employment context, for example, a wide range of questions on employment applications and in job interviews are prohibited or restricted, covering age, race, religion, national origin, disabilities, health problems and medical conditions.

One example of a recently added protected category is genetic discrimination. Genetic information gathered from some subjects can demonstrate an association between a racial or ethnic category and certain genetic dispositions. Once this connection is made, it can be used to make predictions about all members of the racial category, not just those who participated in the data collection.[68] Genetic screening can detect susceptibility for certain disorders such as cancer, Alzheimer's disease and diabetes, and this information could then be used to deny insurance or employment to people.

One result of this concern about the misuse of genetic information was a federal law, the Genetic Information Nondiscrimination Act (GINA), which prohibits U.S. insurance companies and employers from discriminating on the basis of information derived from genetic tests.[69] Under this new law, insurance companies can reduce coverage or increased prices based on information about an applicant's genetic code. Employers cannot take adverse action against employees or potential employees based on genetic information. Neither can they require that a person take a genetic test as a condition of obtaining insurance or getting a job.

Invidious discrimination is illegal, but it might be possible to use statistical techniques to make connections that make it possible in an indirect fashion. Some commentators have argued that allowing eligibility decisions to be made on the basis of statistical information such as credit card transaction history, criminal histories, online browsing patterns and the like would have the beneficial result of blocking direct or indirect invidious discrimination. For example, if an employer could consult a data base of criminal history, then he would be more comfortable hiring an African American who had no criminal history. If employers were not allowed to

[68] Zarsky, p. 46
[69] Public Law 110–233—May 21, 2008 122 Stat. 881

consult such a data base, they would be more likely to fall back on the "old standby" of invidious racial discrimination.[70]

One response to this has been that the patterns embodied in the data can themselves be problematic. This can be so in that they simply reproduce the invidious discrimination. A nationwide pattern of hiring according to criminal history, for example, would reproduce the unequal pattern of African American criminal arrest and convictions records.[71] A more worrisome possibility, however, is that mere patterns in data might be complex statistical proxies for the suspect categories of ethnicity, race and religion.

2. Group injury

In a related way, groups can suffer a harm based upon information externalities. Consider class rankings. If students are allowed to disclose their class ranking to admissions officials or employers, the best students will disclose. Even if other good students try to conceal the information, the fact that they do not reveal their ranking allows those making the eligibility decision to infer that they are not in the top rank. The result for the school will be a drop in the average quality of their placements. As a result of considerations like this, most private high schools and over half of public schools no longer report student class rankings as part of the college admission process because they feel it disadvantages those who are left out of the top rankings.[72]

There is nothing intrinsically improper about making admission decisions on the basis of class rankings, but it helps only the very top students and hurts the rest. A private institution seeking to benefit its members generally might chose to restrict information flow of this kind. Fully informed individual choice about whether to reveal class rankings would allow the top students, rationally, to reveal their top status, thereby revealing, to their detriment, the lesser ranking of the remaining students.

Similar group harm can result from investigations into specific racial or ethnic groups. When scientists were seeking to conduct medical studies of Ashkenazy Jews in the 1990s to determine whether the group's genetic inheritance was linked to specific diseases, there was concern that the results could be used to "cast a shadow over the entire ethnic group."[73]

---

[70] Lior Strahilevitz, "Privacy versus Antidiscrimination," University of Chicago Law Review, Vol. 75, 2007; U of Chicago Law & Economics, Olin Working Paper No. 349; U of Chicago, Public Law Working Paper No. 174. Available at SSRN: http://ssrn.com/abstract=1003001 (arguing that more information about bankruptcies, criminal records, and sex offenses should be made public as a way to make sure that employers do not use inaccurate statistical information to profile potential employers and that more accurate information might hurt the guilty but it will protect the innocent.)

[71] Nissenbaum, p. 209. Her additional claim that mere patterns in data should not be used for eligibility decisions unless supported with "underlying theories of causation" might prevent useful predictive inferences. It seems that what she is really getting at is the worry mentioned in the text that the complex patterns detected in data might simply serve as proxies for the suspect categories of race, religion and ethnicity.

[72] Alan Finder, "Schools Avoid Class Ranking, Vexing Colleges," New York Times, March 5, 2006. At http://www.nytimes.com/2006/03/05/education/05rank.html

[73] Simpson Garfinkel, Database Nation, O'Reilly, 2000, (Garfinkel) p. 190.

Individual consent could be solicited and obtained, but the effects of the studies would extend beyond the data subjects and apply to the entire group. Other individuals in this group might experience negative privacy externalities in the form of invidious discrimination. Individual consent could not respond to this potential for harm.

It might be appropriate for a group representing the group to be consulted prior to allowing the study to proceed, rather than seeking only individual-level consent.[74] Ultimately, some of the harm that such studies could produce such as discrimination in employment was outlawed by the 2008 Genetic Information Nondiscrimination Act.

Groups have an interest in the outcome of information revelation that might be distinct from the interests of the individual members of the group. This kind of group harm cannot be prevented by fully informed individual choice, but can be addressed by institutions or organizations action on behalf of the group as a whole.

3. Inefficient Product Variety

Information about consumers can sometimes be used to change market dynamics in ways that might harm consumers overall. This can happen when the collection and use of personal information leads indirectly through a series of intervening steps to market dysfunctions. One of these dysfunctions is inefficient product variety. For example, when mass marketing and production has substantial scale economies and there is little taste for variety, the introduction of more targeted marketing schemes based on more detailed information about consumers might reduce overall welfare. Studies have shown that consumers are aware of and take an interest in these market effects of information sharing practices. Even when individuals have the ability to refuse data collection requests, if enough other people go along with the information collection and use scheme, the economic damage is done.

Product variety is often thought of as an unmixed blessing.[75] But analysts have isolated cases where there is inefficient product variety. In such a case, a market starts with the provision of a generic product like a general interest newspaper whose production and marketing costs are characterized by substantial scale economies. Then the market shifts to a market with two products – the old generic product and a new specialized product such as a pure financial newsletter. The new product is slightly better for consumers who value only financial news, but the older generic product becomes more expensive as scale economies are lost. The welfare gains and loses are ambiguous, since the new entrant does not compare the gains to the new

[74] This was done in the case of genetic studies on Navajos, for example. See Garfinkel p, 193.
[75] Product variety is often considered and defended in the context of price discrimination. See for example Tom Leonard and Paul Rubin, In Defense of Data: Information and The Costs of Privacy, Technology Policy Institute, May 2009 p. 31 available at http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf

consumers of the financial newsletter to the losses of the old consumers of the generic newspaper. Luc Wathieu describes this situation:

> "When an entrant uses a fine access system to target a specific consumer type, scale economies are dismantled and the remaining consumers suffer from an externality. This mechanism can lead to these consumers being excluded or face with a high-price customer offer that constitutes a loss of surplus and signals the end of benefits customarily associated with mass marketing."[76]

Privacy is relevant to this dynamic because information about the preferences of consumers that is voluntarily revealed to marketing firms is a key element in determining whether the new product should be introduced. The privacy concern has to do with those who do not benefit from firms being better informed about the preferences of different consumer types. They have an interest in not sharing this kind of information. Even if they understand the situation perfectly and chose to withhold information so as to frustrate the development of inefficient product variety, the survey responses or other disclosures from those who would benefit from the new product would reveal the necessary information.

The key thing from the point of view of whether consent to sharing information is sufficient to avoid privacy harms is that it doesn't matter whether they can foresee this use of information. Assume perfect understanding of the implications of gathering information for targeted marketing. Those who would benefit from this change will reveal the information in the full knowledge that they will benefit. This allows an adverse implication regarding those who do not reveal their preferences.

The problem is often viewed as giving people control over the information that could be used to target them. If they have that control, and voluntarily give it up, what could go wrong? The possibility of inefficient product variety shows that something could still go wrong even when consumers have perfect control over information about their preferences. Those who would gain from product variety will reveal information that will help them. Those who would lose will remain silent, but enough market information is available to introduce the product even if the losses outweigh the gains.

One study by Wathieu and Friedman shows that consumers are sensitive to this possibility that information about them will be used to change market cost structures in ways that disadvantage them.[77] The specific scenario used to evaluate these indirect privacy concerns had to do with an affinity marketing program described as follows:

> "As a service to its members your college alumni association has negotiated a special deal with a well-known car insurance company. The insurance company

[76]Luc Wathieu, Marketing and Privacy Concerns, Working Paper. Harvard Business School, 2007 p. 7
[77] Luc Wathieu and Allan Friedman, "An Empirical Approach to Understanding Privacy Evaluation," HBS Marketing Research Paper No. 07-075 April 2007 (Wathieu and Friedman) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=982593

> will use data (including members' name and contact information) on a onetime basis to offer alumni (via a mail and phone marketing campaign) an alumni association endorsed deal featuring first-class service levels and a 30% discount on annual insurance premiums. Based on certain parameters specified by the insurance company, data for 20% of the alumni have been transmitted to the insurance company and all of these alumni are about to be offered the deal. At this point it is still unknown whether you are among the beneficiaries of this deal.[78]

The indirect privacy concern associated with this scenario is that rates for ordinary drivers could go up if insurance companies find increasingly effective ways to target safe drivers. Two thirds of the experimental subjects were somewhat concerned about this arrangement. Most of them wanted the arrangement reviewed and approved or rejected by the Board of Alumni and 53% of the respondents would vote to reject this deal themselves. In an alternative scenario, respondents are told that they will not get the deal and their information will not be shared, but this did not produce a decline in their privacy concern.

Studies like this suggest that consumer concern about privacy cannot be resolved simply by giving people the chance to opt out of information sharing arrangements. People seem to understand that they can be harmed by information sharing arrangements even when they have the ability to refuse to participate in them.

4. Restricted Access

Some commentators have noted that tracking of online behavior can result in restricted options. Marty Abrams describes the situation where "a consumer's vision and choices are limited by his or her digital history and the analytics that make judgments based on that digital history" as "boxing."[79] The idea is that a person's ability to gain access to the full range of goods and services is limited by a service provider's perception of him as a customer of a certain kind. Only certain kinds of products, services or media content will be provided to him. Despite all efforts, he remains trapped by his history.

Sometimes this boxing has to do with credit worthiness and there is nothing to be done about it. Sometimes it operates to his benefit, as when he gains miles in a frequent flier program. But when it operates to restrict access to what is available, it is no longer desirable. Consumers want at some point to say, as Abrams puts it, "Stop the personalization. I want to see the whole picture." The key is not to provide extra choice at the point of data collection, but to have further choice later on that will help to mitigate the harm.

---

[78] Wathieu and Friedman, p. 3

[79] Marty Abrams, Boxing and Concepts of Harm, Data Security Law Journal, September 2009 available at http://www.hunton.com/files/tbl_s47Details/FileUpload265/2692/Boxing_and_Concepts_of_Harm_Abrams_9.09.pdf

Data profiling can produce this result, even when the data for the profiling comes from another person. Zarsky outlines an example. One customer goes to a website, shares personal demographic information and zip code and buys high-priced low-quality products. He is put in the category of customer who should be shown only high-priced low-quality products. A customer with a similar demographic and zip code visits the same website and is put in this same category. He suffers the same restricted access to the website's goods, despite having purchased nothing and provided the website with only demographic information and address.[80]

As Zarsky notes, even if the original visitor is compensated for sharing information, the damage is to an external third party who had no connection to the original transaction. They fit a pattern created by analysis of data from others. Regulating the original transaction which collected the information is not the key to resolving this problem. It is the use of the information that creates the harm.

5. Price Discrimination

Price discrimination occurs when firms charge different consumers different prices for access to the same good or service. Economists distinguish first, second and third degree price discrimination. In first-degree price discrimination, the firm gathers as much information as possible about potential customers in order to assess demand. They are seeking to determine how valuable the good or service they sell is to these potential buyers so as to charge them the highest possible price they are willing to pay. This clearly involves extensive information gathering and profiling of specific individuals and is the form of price discrimination that raises the most questions about privacy harms.

In second degree price discrimination, the firm does not ascertain demand directly by gathering information about individual. Instead, they offer different prices for different versions or different quantities of the same product. The idea is that these purchasing decisions will reveal their preferences. The different prices for the different versions of the same good or service cannot be explained by differences in the costs involved. Instead, the differences are meant to appeal to different intensities of demand. As in first-degree price discrimination, the point is to extract more revenue from those customers willing to pay more than an average price. It can be controversial. For example, products that have certain functions deliberately disabled in order to appeal to less affluent customers have drawn strong protests. But second-degree price discrimination raises fewer questions about privacy harm.

In third-degree price discrimination, the seller does not know the purchasing power of individual buyers, but is able to separate them into groups that correspond roughly to their wealth

[80] Zarsky p. 43

or eagerness. Classic examples are student and senior discounts.[81] Some information about people is needed to engage in third-degree price discrimination, but it is usually large demographic categories or market segments. As the segmentation moves toward personalization, however, this type of price discrimination verges on first-degree.

Price discrimination is not always possible, but can take place only under certain market conditions. The seller has to have some degree of market power. Otherwise, the targets of higher prices could simply go to another supplier who would be willing to charge just the average market price. That is why price discrimination could occur under monopoly telecommunications conditions and in railroad networks with captive shippers. Odlyzko shows that the railroad industry practiced widespread price discrimination which led to government regulation of its prices.[82]

Second, the seller must have enough information to put customers into market segments that differ by the willingness to pay for the good or service. This can be done effectively only with good information about specific customers or classes of customers. Third, the seller must be able to control arbitrage. If customer who pay little for a good or service can resell it to customers who assessed as high-price customers, the price discrimination will be eroded.[83]

Price discrimination can be good or bad from a social welfare point of view. Price discrimination usually raises the profits of the firm that can engage in it. But it can be inefficient. It can reduce overall social welfare. Compared to a situation of a uniform market price, the gains to those receiving a lower discriminatory price might be less than the losses to those who pay a higher price or forego consuming the good altogether. This can happen for example when there are very few people in the group that gains, and a substantial number in the group that loses, Alternatively it could happen if the groups are of similar size, but the gains to those in the winning group are small, while the harm to the losing group is substantial.[84]

Law and policy vary substantially in the approach taken to price discrimination, as befits the indeterminacy of its social welfare implications. There is no good guide for policy makers as a general matter. As Fisher sums it up:

> "…price discrimination is good in some setting and bad in others. Somewhat more specifically, the merits of the practice are affected by myriad variables, including the shape of the submarkets that it permits separating, the character of the criteria used to

[81] William W. Fisher III, "When Should We Permit Differential Pricing Of Information?" 55 UCLA Law Review 1 (2007) (Fisher) p. 7
[82] Andrew Odlyzko, Privacy, Economics, and Price Discrimination on the Internet, ICEC2003: Fifth International Conference on Electronic Commerce, N. Sadeh, ed., ACM, 2003, pp. 355-366. Available at http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf
[83] Fisher, pp. 6-7
[84] Fisher, p. 22.

divide those groups, its transparency, and public attitudes toward specific forms of the practice."[85]

Price discrimination is unpopular. Consumer reaction to Amazon's attempt to use information about repeat customers to charge them a higher price, thereby punishing loyalty, was so uniformly negative that the practice was abandoned.[86]

In a survey of public attitudes, Turow and his colleagues found that people "overwhelmingly object to most forms of behavioral targeting and all forms of price discrimination as ethically wrong."[87] The study found that:

- 76% agree that "it would bother me to learn that other people pay less than I do for the same products."
- 64% agree that "it would bother me to learn that other people get better discount coupons than I do for the same products."
- 66% disagree that "it's OK with me if the supermarket I shop at keeps detailed records of my buying behavior."
- 87% disagree that "it's OK if an online store I use charges people different prices for the same products during the same hour."
- 72% disagree that "if a store I shop at frequently charges me lower prices than it charges other people because it wants to keep me as a customer more than it wants to keep them, that's OK."

Part of the reason for its unpopularity is the sense that the bargaining situation has been altered in an unfair way. As many have noted, information in the hands of the powerful is a more effective tool than in the hands of the weak.[88] The information used to price discriminate is not symmetric. The seller knows more about the buyer than the buyer knows about the seller. As Marc Rottenberg notes, this asymmetry can exacerbate differences in bargaining power:

> "In bargaining, no one wants to give up their 'reservation' price to the other side. With profiling, the consumers give up the privacy of their reservation price, but the seller doesn't. So it changes the power in the bargaining, against consumers."[89]

For our purposes, the key question is whether price discrimination involves privacy harms. Here the consensus of commentators seems clear:

---

[85] Fisher p. 37

[86] David Streitfeld, "On the Web, Price Tags Blur; What You Pay Could Depend on Who You Are," Washington Post, Sept. 27, 2000

[87] Joseph Turow Et Al., Open To Exploitation: American Shoppers Online And Offline, Annenberg School of Communications, Departmental Papers, June 2005, *available at* http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/Turow_APPC_Report_WEB_FINAL.pdf p. 4

[88] Nissenbaum, p. 211.

[89] Marc Rotenberg, Fair Information Practices and the Architecture of Privacy: *(What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 available at http://stlr.stanford.edu/pdf/rotenberg-fair-info-practices.pdf

- "Policymakers could consider whether price discriminating firms are violating consumers' privacy interests"[90]

- "...price discrimination is bad if it fosters invasions of privacy."[91]

- "Privacy intrusions serve to provide the information that allows sellers to determine buyers' willingness to pay." [92]

The concern can be described in more detail as follows:

> "This is an especially serious worry with respect to first-degree price discrimination. In order to charge each customer close to the maximum amount that he or she would be willing and able to spend, sellers need to know a good deal about individual buyers. Useful information includes their incomes, wealth, tastes, purchasing habits, and credit histories. The value of that information to discriminating sellers may induce them to create and then exploit channels for gathering and then aggregating data about their potential customers. That, in turn, may exacerbate the extent to which the information technology revolution is already encroaching upon traditional conceptions of privacy.[93]

But this description of the privacy harm is entirely circular. The gathering and aggregating of data about potential customers is violates privacy rights, goes the argument, because it leads to price discrimination, which for the sake of the argument is assumed to be injurious. But then the argument turns on its tail and declares that price discrimination is injurious because it rests on the privacy harm of gathering and aggregating data about potential customers.

It is important to be clear about what is the cause and what is the effect in the privacy harm connected to price discrimination. The harm in this case is the price discrimination that results in a net loss of social welfare. As we have seen, it is sometimes hard to determine when a price discriminatory practice is harmful. Economic theory is not a reliable guide in this area. But even if the information gathered for the discriminatory pricing has been gathered with full notice and consent, the harm can occur. As we have seen in other cases, information gathering and analytic techniques can produce information about one set of data subjects that is derived from another set. Informed consent cannot protect against this kind of information leakage. When

---

[90] Matthew A. Edwards, Price and Prejudice: The Case Against Consumer Equality in the Information Age, 10 Lewis & Clark L. Rev. 559, 593 (2006) at http://legacy.lclark.edu/org/lclr/objects/LCB10_3_Edwards.pdf

[91] Fisher p. 36

[92] Andrew Odlyzko, Privacy, Economics, and Price Discrimination on the Internet, ICEC2003: Fifth International Conference on Electronic Commerce, N. Sadeh, ed., ACM, 2003, pp. 355-366. Available at http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf p. 1

[93] Fisher pp. 36-37

there is a privacy harm resulting from price discrimination, it can be an external harm, created by the leaky character of information.

IV. THE UNFAIRNESS MODEL FOR PRIVACY POLICY

A. Introduction.

These examples of invidious discrimination, group harm, inefficient product variety, access restrictions, and price discrimination mean that when information leaks there can be negative privacy externalities. They suggest that something other than disclosure is needed as the centerpiece of privacy policy. Policy makers need to evaluate directly the outcomes of information use, and not focus solely on creating an ideal information collection process. This is not to say that rules for information collection are unimportant. But in order to device an adequate information collection process, policy makers will have to evaluate information use.[94]

Two examples illustrate this extra dimension. Consider information security. People do not ask merchants to tell them what level of security they provide when transfer personal information for a transaction. They simply expect it to be kept safe and secure. They do not want to control the information. They do not want to know what they do to keep it secure. They just want the data collector, and those to whom he passes it on, to protect it. If they fail to keep it safe and secure, people expect that this unfairness will be remedied by government, or that they will have recourse to legal proceedings to hold those responsible to account. While people certainly expect to be notified if a security breach involving their personal information has exposed them to the risk of harm, disclosure of security precautions before the fact is simply irrelevant. People do not shop based on "security" ratings anymore than they travel on bridges based on whether that have a small, medium or large risk of collapse. Finally people do not think that those who have failed to protect the information entrusted to them to escape all legal liability on the grounds that they really had not promised to protect the information.

The second example is consumer financial protection. For years, federal financial regulators implemented the statutory prohibition on unfair and deceptive acts and practices through disclosure requirements. As long as the terms of a financial product were clearly and conspicuously disclosed to consumers, the product itself could be anything at all. The recent financial meltdown has revealed the shortcomings of this disclosure approach. The Congress and the federal regulators reversed course in 2008 and 2009 by banning some credit card practices. Issuers are no longer able, for example, to apply new interest rate changes to old credit card balances – even if they tell consumers in advance. The practice itself is so unfair that no amount of disclosure could render it legitimate.

Privacy policy needs to supplement informed consent with that kind of thinking. Some uses of information are damaging to consumers, they are hard for consumers to avoid on their

[94] See Zarsky p. 32 ("Solutions should protect the public from dangerous uses, not from mere surveillance.")

own and they have no offsetting benefits. Unfair information practices of this kind should be prohibited, not simply disclosed. Examples might the use of medical information or information about sexual preferences to target advertisements to vulnerable people; the use of information to commit fraud or to engage in invidious discrimination; posting social security numbers or other access identifiers online; tracking everything people read or everywhere web users go on line and keeping these files forever when they can be subpoenaed in civil litigation or sold to the highest bidder.

This focus on prohibiting practices might seem extreme. Why should any uses of information be impermissible? But the opposite conclusion has already been reached in the past. That is, policymakers have concluded that certain uses of information are so important the individual choice simply cannot be allowed. People are not given the right to opt out of collection of information by credit bureaus because to do so would be to defeat the purpose – those with bad credit history would opt out and there would be no good information on bad credit risks. Under existing financial privacy rules, people cannot restrict the use of information about them for fraud prevention purposes. The idea that some uses of information are so unfair that they should be restricted is just the other side of the coin of the idea that some uses of information are so beneficial that individual choice cannot block them.

B. Financial Consumer Protection

In May 2008, various banking agencies proposed rules addressing certain unreasonable practices in connection with consumer credit card accounts and overdraft services for deposit accounts.[95] Before the rules could come into effect, however, Congress intervened and codified many of them in the Credit Card Accountability Responsibility and Disclosure Act of 2009.[96]

The rules represented a dramatic change from the traditional way of regulating unfair actions in the financial service industry. Prior to these decisions, the banking agencies required substantial disclosure as a preventive remedy against unfair actions. If consumers were fully informed of the terms and conditions of a credit or debit card product, then they could take steps to protect themselves by refusing to do business with companies whose financial products were too expensive, too hard to understand, or too tilted toward the interests of the financial service company.

One of the banned practices was universal default. Under this practice, a credit card company raises a consumer's interest rate if the consumer makes a late payment on an account with a different creditor, such as a cable company or a cell phone company. The harm was the retroactive application of a higher interest rate to an existing balance. Information from other creditors could be used to increase rates on future balances, but not on existing balances.

[95] 73 FR 28904, May 19, 2008
[96] Public Law 111–24, 123 Stat. 1734 (2009).

The banking agencies were very clear that disclosure would not be enough:

> The Agencies are concerned that disclosure alone may be insufficient protect consumers from the harm caused by the application of increased rates to pre-existing balances. Accordingly, the Agencies are proposing to prohibit this practice except in certain limited circumstances. [97]

Another practice that was banned was double cycle billing. This occurs when the finance charge on an outstanding balance is computed based on balances in earlier billing cycles, not just on the balances in the most recent billing cycle. This practice was so counter-intuitive and hard to understand that the agencies found that no amount of explanation or disclosure could render it fair.[98]

C. Reasonable Information Security

In 2005, the Federal Trade Commission began to charge companies with acting unfairly by failing to provide reasonable security. In the case it filed and settled against BJs the FTC listed the practices that did not provide reasonable security, including

- Failed to encrypt consumer information when it was transmitted or stored on computers in BJ's stores;
- Created unnecessary risks to the information by storing it for up to 30 days, in violation of bank security rules, even when it no longer needed the information;
- Stored the information in files that could be accessed using commonly known default user IDs and passwords;
- Failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and
- Failed to use measures sufficient to detect unauthorized access to the networks or to conduct security investigations.[99]

The specificity of these practices relates to the use by the FTC of an industry standard, the Payment Card Industry Data Security Standard, as a guide to best practices in the industry.[100] The claim was that these practices taken together amounted to a failure to take reasonable precautions to keep cardholder information safe and secure. As a result of this failure, issuing banks suffered financial losses from fraud, card reissuance, and monitoring and notification costs. Cardholders suffered inconvenience, worry and time loss dealing with cards that needed to be replaced. Claims against BJs amounted to $13 million. The settlement required BJ's to

---

[97] 73 FR 28904, May 19, 2008 at 28917
[98] 73 FR 28904, May 19, 2008 at 28939
[99] *See* FTC Press Release, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), *available at* www.ftc.gov/opa/2005/06/bjswholesale.shtm
[100] See the PCI standard at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml For a discussion of the use of the PCI standard in FTC reasonable security cases, see Mark MacCarthy, Payment Card Industry Data Security Standard, in Proskauer on Privacy, Practicing law Institute, 2009

implement a comprehensive information security program and obtain audits by an independent third party security professional every other year for 20 years.

By 2008, the FTC had taken actions against twenty companies for failure to practice reasonable security.[101] In one of the most recent cases involving TJX case, among the problems the FTC noted were:

- storing and transmitting personal information in clear text
- failing to use readily available security measures to prevent unauthorized access to its in-store wireless networks,
- not requiring the use of strong passwords or different passwords to access different programs, computers, and networks,
- failing to use readily available security measures such as a firewall to limit Internet access to its computers,
- not employing sufficient measures to detect and prevent unauthorized access, including failing to update anti-virus software, and not following up on security warnings and intrusion alerts.

These violations of reasonable security also related to the PCI data security standard. The settlement required TJX to establish and document a comprehensive information security program and obtain an audit every two years for the next 20 years.[102]

In each of these cases the agency found that specific practices were unreasonable and ordered that they be stopped and replaced with a reasonable set of information security practices based on a widely accepted industry standard. The remedy for the unreasonable actions was not a notification requirement.[103] The company was not required to inform its customers of the detailed steps it was taking to secure the cardholder information against unauthorized use. It was not required to obtain consent from them that they accepted the information security practices put in place. Instead, the agency simply mandated that the company stop the bad practices and begin the good ones.

---

[101] The latest involved TJX. *See* FTC Press Release, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), (TJX Release) *available at* www.ftc.gov/opa/2008/03/datasec.shtm . Other similar cases the FTC has settled include in addition to BJ's and TJX include DSW, and CSSI. See FTC Press Release, DSW Inc. Settles FTC Charges (Dec. 1, 2005); FTC Press Release, Card Systems Solutions Settles FTC Charges (Feb. 23, 2006).

[102] See TJX release.

[103] Data breach notification legislation is an entirely different response to the data security problem. They require notification both to allow potential victims to take action to protect themselves and to induce companies to protect information so as to avoid adverse publicity. As of April 12., 2010, forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches. See the list maintained by the National Conference of State Legislators at http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

D. The Unfairness Framework

Instead of a framework that relies on notice and choice alone, the unfairness framework creates several categories of information collection and use and varies the regulatory response depending on the category. At one extreme lie those practices involving the collection and use of information that are impermissible even with data subject choice. Call them harmful or impermissible uses of information. At the other extreme stand those practices involving the collection and use of information that are so important that they should be allowed even without data subject choice. Call them public benefit uses. In between lies the realm of choice.

One way to measure the value of the information use is expected social utility, defined as the net social gain or loss discounted by the probability of it occurring. This way of thinking about benefits and harms obviously fits most closely with the economic framework of cost-benefit analysis, which normally involves a quantitative comparison of costs and benefits. But quantification and measurement have to be relative to the type of benefit and harm involved. In many cases, the type of harm involved such as an affront to human dignity or the benefit to human welfare derived from an increase in autonomy and opportunity will be real effects of an information practice that are not amenable to expression in quantitative terms. A qualitative assessment might be all that is possible in many cases.

The focus is social, not individual. The fact that some individuals or groups of individuals benefit or are harmed by an information practice does not automatically mean that it is a social gain or a social loss. The perspective is on what is on balance good for society as a whole. Equity gains or losses have to be taken into account as well to the extent that policy makers reach the judgment that harms or gains to specific groups are worthy of special consideration

Finally, the perspective has to be probabilistic. Existing information practices can be evaluated in part by their actual consequences. But even then an assessment has to be made of the likely evolution of the information practice in the future and how an industry might adjust to any perceived harms. New innovative uses of information have no track record and so the assessment would have to be based on the likely results of adding the new practice to the existing mix of information practices and contexts. The level of uncertainty in these evaluations has to be taken into account when considering any regulatory regime.

The unfairness regime does not ignore the role of informed consent. But it treats informed consent as one regulatory tool among others. Within the unfairness framework, the first step is the provision of information so that consent can be informed. Providing information to consumers can be done in one of two ways: disclosure and notification. Disclosure is the

public acknowledgement of an information collection and use practice.[104] Notification is the provision of this information to a specific individual. [105]

Notice and opt-out would be an appropriate policy response when the information practice in question is closer to the public benefit use. Notice and opt-in would be the appropriate policy when the information practice is riskier, closer to the harmful uses. Easy opt-in choice is especially problematic when an information practice has substantial external information effects that spread the harmful effects beyond those who have chosen to participate in it.

1. Public Benefit Use

Sometimes the use of information is so important to the public that choice should not be permitted. In a recent case, the Center for Disease Control used information from shopper loyalty card to track down the source of a salmonella outbreak. The supermarkets involved gave the information to health officials for data mining only after the shoppers provided their consent.[106] But what if there was no opportunity for consent? Would the supermarkets have been justified in providing the information in any case? Would CDC have been justified in demanding it? The perspective of net social utility would suggest that the answer might very well have been yes.

Cases like this are not hard to find.[107] Public health emergencies or the demands of scientific or medical research sometimes make choice less attractive. In most cases, public disclosure of the data use would be required, although not necessarily individualized notification to the data subjects. To the extent that opting out of these public benefit uses destroys the effectiveness of the use to that extent there is a case for limiting choice.

The detailed discussion of these situations is beyond the scope of this article. Two general conditions seem to call for limitations on informed consent in the context of public benefit uses. One is when getting consent is so expensive that it would render a particular use uneconomic and this use is socially beneficial. Another is when the major value of the information is its completeness. In these circumstances, allowing individuals to opt out of the use would prevent the use altogether or substantial limit its benefits.

---

[104] Disclosure can be accomplished by a public description of the information collected and how it is used. Privacy policies posted on an internet site are one example. They are made available to all and apply equally to all.

[105] Individualized notice is the transmission to customers of detailed information about a company's collection and use of information. Each customer must receive a separate notification. GLBA financial privacy notices are examples as are the individual notices sometimes required under data breach notification laws. Individually transmitted credit card disclosures are a third.

[106] David Mercer, CDC uses shopper-card data to trace salmonella, Washington Post, March 10, 2010 at http://www.washingtonpost.com/wp-dyn/content/article/2010/03/10/AR2010031002389.html

[107] Amitai Etzioni documents many of them ranging from trade-offs of privacy versus security to limitations on choice in the context of medical research and public health. See generally Amitai Etzioni, The Limits of Privacy, Basic Books, 1999.

One example of this is the use of information for eligibility decisions. In the United States, credit bureaus are able to compile full files on individuals, containing negative information about defaults and other non-payment, as well as positive information about their history of successful repayment. These organizations are able to combine information from large numbers of creditors, who furnish repayment information, and perform sophisticated analytics on the data to predict credit and other risk. These systems have substantial advantages compared to a situation in which each individual creditor has to rely solely on its own information about credit risk and compared to situations in which only negative information is furnished to credit bureaus.[108]

The successful implementation of this system of full file reporting does not allow for consumer choice. Consumers provide information to creditors in the context of the repayment of loans. These creditors then furnish this information to credit reporting agencies without providing consumers with any opportunity to opt out of this reporting. This is necessary for two reasons. First, it is needed to avoid adverse selection.[109] If consumers could opt out, then only those with good repayment histories would allow their creditors to furnish the information to credit bureaus for aggregation and analysis. Creditors using credit bureaus for risk analysis would have good information only on good credit risks. Second, assuming that those who refused to supply information were all equally bad credit risks is not a sufficiently granular response. Some of those who would not allow credit reporting are more worthy of credit than others, but the system would not generate enough usable information about these individuals to distinguish them from others less worthy of credit. Creditors would most likely react to the absence of information about people who refused to furnish it by simply credit to all of them, even though many of them were in fact credit worthy.

Granting a choice to individuals to control the flow of information out of credit bureaus does not suffer from this difficulty. Many states (47 plus the District of Columbia) have reacted to the increase in reported identity theft by passing laws that allow people to put a freeze on their credit report.[110] The idea is that a creditor will not be able to obtain a credit report with getting affirmative permission from the data subject. Identity thieves will have a harder time opening an account in a victim's name if creditors such as credit card companies have to contact the victim first before opening the account. This does not affect the reporting of information into the file; instead, it imposes important protections on the provision of a file to a potential creditor.

The lack of individual choice in this area does not mean a lack of consumer protections.[111] The analysis of information compiled in the credit reports is not restricted, but the

[108] See John Barron and Michael Staten, The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience 2000, available at http://www.privacyalliance.org/resources/staten.pdf
[109] Beales and Muris, pp. 116-117
[110] See Consumers Union Guide to Security Freeze Protection for a list of states that have passed credit report freeze laws available at http://www.consumersunion.org/campaigns/learn_more/003484indiv.html
[111] 15 U.S.C. § 1681 et seq. available at http://www.ftc.gov/os/statutes/031224fcra.pdf

use of the information and analysis is. Permissible purposes are limited to credit, employment, and insurance. Use for other activities such as marketing is not permitted. However, the "header" information that links the report to an individual and which contains name, address, phone number, date of birth and social security number can be and is sold to companies for a wide variety of purpose unconstrained by the permissible purposes limitation. Data subjects have transparency rights, including the right to access and correct the file and to receive a free copy of it each year. There is accountability in the use of the information through the mechanism of an adverse notice whenever an action is taken to deny credit or employment to a person based on the information in the file.[112]

The balance between publicly beneficial use of consumer information and consumer protection is often a matter of dispute and it can and should be adjusted from time to time. For our purposes, the point is that the FCRA is an example of how to regulate a publicly beneficial use of information without the mechanism of individual choice, but with consumer protections.

2. The Realm of Choice

There are several different kinds of disclosure, notice and choice regimes that make it more or less likely that people will engage in an information practice. At the one extreme, policy makers could require individualized notice, a default of no use of information and a difficult or costly opt-in process. This policy choice is a "nudge" to consumers not to engage in the practice.[113] At the other extreme, policy makers could allow a more relaxed notice and choice regime for an information practice that nudges people into accepting it. Notice requirements might be restricted to generalized disclosure of the information practice, rather than individualized notifications. Firms and institutions would be allowed to engage in it unless told to stop by the data subjects themselves, and there might be no obligation to spend resources to make opt-out mechanisms easy or convenient for consumers. In between, there are various ways to structure a disclosure, notice and choice regime. Table 1 presents one illustrative example of how such a range of options might be structured.

How should policy makers determine what kind of choice framework to provide for an information practice? In the unfairness framework, there is an interaction between the evaluation of the information practice and the kind of disclosure, notice and choice involved. One way to apply the framework, for example, would be to require individualized notice, a default of no use of information and a difficult or costly opt-in process when the dangers associated with an information use are high.

---

[112] This requirement was recently updated through the issuance of a final rule requiring notice for risk-based pricing decisions derived from credit reports. See Federal Trade Commission and Federal Reserve Board, "Agencies Issue Final Rules on Risk-Based Pricing Notices," December 22, 2009 available at http://www.ftc.gov/opa/2009/12/rbpricing.shtm

[113] See Richard Thaler and Cass Sunstein, Nudge, Penguin Books, 2009 for a discussion of the use of policy defaults as a way to provide an incentive to individuals to move in a direction that best satisfies their long-term interests. See also Richard Thaler and Cass Sunstein, "Libertarian Paternalism Is Not An Oxymoron," 70 University of Chicago Law Review 1159 (2003) for arguments in favor of setting default rules provide incentives for certain behaviors rather than imposing binding prohibitions or mandates.

The dangers associated with an information practice would include the extent to which information externalities were present. Easy opt in is especially problematic when information externalities are present and the practice is likely to be harmful. In these cases, people cannot protect themselves from harm by refusing to disclose. If enough other people disclose, the harm is done. In these cases, it would be even more important for policy makers to make it difficult for people to engage in the practice by imposing a rigorous choice requirement, because their decision to engage in it has external negative effects on other people.

The default setting that the information practice in question can only take place with the affirmative express consent of the data subject is appropriate when policy makers want to nudge consumers in the direction of not furnishing information for that purpose. Firms and other institutions that want to engage this practice are not forbidden to do so, but they must first provide an adequate description of what the information practice involves and obtain consent from the data subjects. The process itself of providing the information to potential consumers is often expensive and can itself act as a barrier to the economic provision of the service. And given fact that people rarely change defaults, it is likely that few people will chose to use the service.

In contrast, when information use is reasonably likely to produce pubic benefits, the notice and choice regime needs to nudge people into accepting it. Notice requirements might be restricted to generalized disclosure of the information practice, and firms and institutions would be allowed to engage in it unless told to stop by the data subjects themselves. The opt-out mechanisms might not have to be easy or convenient for consumers. The idea would be that only consumers who were very concerned about the practice and willing to go to substantial lengths to opt out of it would take the trouble to take advantage of the opt-out opportunity. When negative information externalities are small or positive, policy makers can be even more confident that an opt-out is the right policy choice.

An attempt can be made to avoid an assessment of the social value of an information practice by talking instead about the type of information involved. If information is "sensitive" then consumers have to be given a greater degree of control. But this inevitably creates overly broad rules such as a rule requiring affirmative express for all uses of financial information. To remedy this defect of over breadth, a series of exceptions from the rule can be crafted, such as for operational or fraud uses.[114] But a list of exceptions cannot be flexible enough to cover the possible information uses that might provide significant benefits. The result is that as a practical matter the opt-in rule for information uses involving financial information or for "sensitive" information generally acts as a barrier to innovation in that area.

To ensure that information is usable for consent, the FTC can use it authority to prevent deceptive practices. For example, the activities of Sears were the subject of an FTC enforcement action under its deception authority. In this case, the FTC ruled that disclosure was inadequate,

[114] This is the approach taken by the draft Boucher bill and suggested by the FTC draft principles.

and it required an affirmative opt in for the kind of data collection the company was contemplating. The disclosure had to be clear and conspicuous and presented at the time when the information would be useful for decision making, not buried in the details of an unread privacy policy.[115] There is some indication that the FTC is will increasingly use its deception authority to regulate the quality of disclosure and choice provided.[116]

3. Impermissible Uses

A wide variety of harms can be considered in this category. The very general concept involved is that there are uses of information, which, on balance, are so harmful for society that they are not allowed. This general concept does not specify in particular cases which harms fall into that category, nor does it describe a procedure for determining what falls in that category. The preceding sections discussed possible harms involving invidious discrimination, inefficient product introduction and price discrimination, without making a judgment about whether they are so harmful that they should be restricted. But the discussion indicates that at least some information practices are harmful.

Many harms are tangible and measurable. Loss of life and limb are measurable harm. Loss of property and monetary damages are tangible. The loss of employment, credit or insurance is a measurable harm. The increased price for credit derived from risk-based pricing is a tangible harm.[117] The loss of reputation is a tangible harm that can sometimes be measured. Businesses interested in preserving their brand take concrete and practical steps to avoid or minimize reputational risk. The damage to credit worthiness from identity theft is a measurable harm, as is the time and inconvenience needed to restore the perception of credit worthiness.

Harm can be probabilistic. Even if the actual harm never materializes the additional likelihood of harm is itself damaging. Extra risk of harm is also a harm. Increased risk of death or physical assault represents a loss of well-being. The increased risk of identity theft is a measurable harm. Greater exposure to the loss of property and monetary damage are tangible harms.

---

[115] Federal Trade Commission, Complaint In the matter of Sears, September 9, 2009 http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf

[116] See the recent statement from FTC Chairman Jon Leibowitz: "You can't take away consumer rights by burying them in the fine print," Leibowitz said. "That would be an unfair or deceptive act or practice under the FTC's bread-and-butter statute and a violation of the FTC act." Bob Herbert, FTC Privacy Review Could Mean Trouble for Online Marketing, Advertising Age, April 19, 2010 at http://adage.com/columns/article?article_id=143343

[117] Risk-based pricing refers to the practice of setting or adjusting the price and other terms of credit provided to a particular consumer based on the consumer's creditworthiness. Pursuant to the Fair and Accurate Credit Transactions Act of 2003, the FTC and federal banking regulators require a creditor to provide a consumer with a notice when, based on the consumer's credit report, the creditor provides credit to the consumer on less favorable terms than it provides to other consumers. Prior to the 2003 revision of FCRA, this action did not count as an adverse action requiring notice. See Federal Trade Commission and Board of Governors of the Federal Reserve System Agencies Issue Final Rules on Risk-Based Pricing Notices, Press Release, December 22, 2009 available at http://www.ftc.gov/opa/2009/12/rbpricing.shtm. The fact that the practice requires an "adverse action" notice reveals that it counts as a quantifiable harm to the consumer involved, even if on balance this business practice does more good than harm.

It is important to specify that harms need not be tangible or quantifiable. Some real harms are hard to quantify. This is the case for the harm of intrusion when telemarketers interrupt normal activities with unwanted telephone solicitations. The insult to dignity experienced when someone examines a data subject's medical or financial records for no good reason except curiosity is also a real but intangible privacy harm. In general violations of people's reasonable expectations of privacy are genuine, but hard to quantify harms.

It might be reasonable to try to operationalize the real, but intangible harm created by mere disclosure of information as the increased risk of a broad, but indeterminate class of more tangible economic harms. If information about the web browsing habits of large numbers of people is generally available to data analysts working for companies seeking commercial advantage, these data subjects might feel exposed and at risk. They might not know exactly what could go wrong, but they have a sense that one or more uses of this data might cause them tangible harm. They might conceptualize this as an insult to dignity, or a restriction on autonomy. At the same time, associated with this intangible affront to dignity and autonomy is the real and perhaps significant risk that their web browsing habits might be used against them. A significant risk of injury is an injury. The intangibility derives from the lack of knowledge of where the injury might come from, but with the understanding that damage of some kind is highly likely.

One standard for determining that a use of information is harmful is the FTC's unfairness standard, discussed in the next session. There might be other criteria from other bodies of law such as civil rights, consumer protection, or competition policy. But one way to evaluate whether a kind of information use is in the category of harmful use is the FTC's unfairness standard.

:

Table 1. Regulation by Expected Social Value of Information Use

		Public Benefit	High Value	Medium Value	Low Value	Low Risk	Medium Risk	High Risk	Harmful	
	Disclosure	Sometimes	Yes	Yes	Yes	Yes	Yes	Yes	NA	
	Individual Notice Needed?	No	No	No	No	No	Yes	Yes	No	
	Default	Use	Use	Use	Open	Open	No Use	No Use	No Use	
	Choice	No opt out	Hard to opt out	Easy to opt out	Easy to change	Easy to change.	Easy to opt in	Hard to opt in	No opt in	

E. The Unfairness Standard

Unfairness is a key concept in understanding how people can be protected from harmful uses of information. There is a substantial case law on the FTC's use of unfairness that can be brought to bear on the question of whether specific acts or practices involving the collection and use of information are unfair. [118] The Congress has codified a standard for unfairness, defining it as taking place when:

> "…the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[119]

The interpretation of this statutory mandate involves the use of a three part test: (1) does the act or practice cause substantial injury to consumers? (2) Can this injury be reasonably avoidable by consumers? (3) Are there countervailing benefits to consumers or to competition? This three part test is essentially a reduction of the concept of unfairness to a cost-benefit test.[120]

The key element is whether the injury is substantial. A substantial injury cannot be trivial or speculative, but ordinarily consists of "monetary, economic or other tangible harm."[121] Emotional distress, mental anguish, loss of dignity and other harms are not ruled out by this criterion, but they must be effects that all or most or reasonable persons would construe as genuine harms. Thus, a finding that unsolicited commercial telephone calls at dinner time were intrusive and caused unjustified emotional harm would not be refuted by claiming that the harm is purely mental, or by showing that it is not universally shared because some people like to be interrupted at dinner. It would be enough to note that most or reasonable people would find such intrusions a source of annoyance and distress.

The unfairness concept of substantial injury is flexible enough to accommodate the intangible "dignity" harms that FTC Consumer Protection Bureau Director David Vladeck's

[118] The history of the FTC's unfairness authority is controversial, and for year congress refused to allow unfairness rulemakings because it did not perceive that the authority was tightly enough constrained. The establishment of the unfairness standard in statute restored the FTC's ability to act comprehensively in this area. For further discussion, see J. Howard Beales, "The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection," 22 Journal of Public Policy and Marketing 192 (2003)
[119] 15 U.S.C. 45(n)
[120] Beales and Muris, p. 132.
[121] May 2008 Proposal at 28908. See also FTC Policy Statement on Unfairness at 3 ("In most cases a substantial injury involves monetary harm...Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair. Thus, for example, the Commission will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers...")

recently described notion of a more expansive view of harm as a potentially intangible concept that goes beyond monetary loss to include violations of dignity.[122]

A substantial injury can be distributed.[123] Information uses that reduce privacy by small amounts for large numbers of people therefore could count as unfair. The familiar problem that privacy can be lost in small amounts is covered by this notion: even if the amount of the privacy harm per person is small the aggregate cost can be very high.[124]

A substantial injury can be probabilistic.[125] If a use of information creates a substantial risk of harm it is substantial injury. Under FTC standards, there is no justification for claiming that no harm was done because the risk of harm did not materialize. A person is worse off if his chances that he will be injured increase even if the harm never transpires. Insurance companies, credit granting institutions and other business enterprises have well-developed ways of quantifying such risks in financial terms, and incorporating them into their accounting systems.[126]

When the FTC acted to require companies to practice reasonable security, they were invoking this probabilistic notion of substantial harm:

> "(the) failure to employ reasonable and appropriate security measures to protect personal information and files caused or **is likely to cause** substantial injury to consumers that is not offset by countervailing benefits to consumers or

[122] Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 4, 2009, *available at* http://www.nytimes.com/2009/08/05/business/media/05ftc.html (quoting David Vladek s saying "There's a huge dignity interest wrapped up in having somebody looking at your financial records when they have no business doing that").

[123] FTC Policy Statement on Unfairness at n. 12 ("An injury may be sufficiently substantial, however, if it does a small harm to a large number of people...")

[124] The unfairness framework thereby responds to the "moral mathematics" concern articulated by Helen Nissenbaum in Privacy In Context (Stanford Law Books, 2009) that each privacy incursion is "a step down the slippery slope" (p. 242) and that some institutional structure must be found to "stop the slide down the slope and prevent society from throwing away privacy in tiny bits." (p. 243)

[125] FTC Policy Statement on Unfairness at n. 12 ("An injury may be sufficiently substantial, however, if...it raises a significant risk of concrete harm.")

[126] Some courts have refused to recognize that the increased risk of a privacy harm is a harm. In Pisciotta v. Old National Bankcorp, a case involving identity theft, the court dismissed a suit by a group of people alleging that the disclosure of their personal information to a hacker had injured them by saying, "(w)ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy." See Pisciotta v. Old National Bankcorp, 499 F.3rd 629, 639 (7th Cir. 2007) In a similar way, in *Allison v. Aetna*, U.S. District Judge Legrome D. Davis dismissed a class action suit against an insurance company whose data base had been hacked, noting that "At best, plaintiff has alleged a mere possibility of an increased risk of identity theft, which is insufficient for purposes of standing, and he certainly has not asserted a credible threat of identity theft," Shannon P. Duffy, Class Action Suit Over Aetna's Security Breach Is Dismissed, The Legal Intelligencer, March 11, 2010 at http://www.law.com/jsp/article.jsp?id=1202446049469&pos=ataglance. It is not clear whether the courts in these cases are dismissing the actual increase in risk as irrelevant or noting that the allegation of increased risk is merely speculative, or asserting that the increased risk is real but not large enough to be significant or substantial. In any case, the FTC's policy of bringing cases for the increased risk of identity theft under its unfairness authority demonstrates that they have the ability to take probabilistic harms into account.

> competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice."[127] (emphasis added)

A second element in the unfairness test is whether people have the ability to protect themselves from the harm through their own actions. Declining to participate in the activity is one way to protect oneself. Sometimes an information practice is harmful, but there are ways to remedy it that do not involve prohibitions. Supplementing market mechanisms with government-supplied or required practical, convenient opt-out choice might be all that is needed. The intrusion harm from telemarketing calls could be addressed in this way. But if an industry practice is widespread there might be no practical alternative. In addition, an unfair feature of a transaction might be so small an element of it that it cannot reasonably be the basis for rejecting the transaction as a whole.

The question of whether consumers can reasonably avoid harm is connected to the notion of privacy externalities we have been developing. As data analytics become more refined, it will be less possible for concealment to prevent the harmful use of information. In more and more circumstances, leaving the decision to share or not to share information to the individual would not protect other individuals. If a person declined to disclose the presence or absence of a particular characteristic, the data collector could still obtain that information indirectly. As we have seen, data collectors and analysts can obtain other information about the data subject either directly or through publicly available or commercial data bases. Using advanced analytical techniques they can often infer with a reasonable degree of probability whether the person had the characteristic. Reasonable efforts by individuals to protect themselves by withholding information might be useless in the context of ubiquitous data collection and powerful analytics.

A third element in the unfairness standard is that the harm is not outweighed by a greater social good. This is essentially a requirement to do an assessment of the benefits of an information practice as well as the costs. The key element here is social good. The compensating benefit need not be distributed to the same individuals who experience the harm. For example, credit bureau information related to a person's repayment of debt can be either positive or negative information. If it is negative, it makes perfect sense for a person to want to conceal it. But Congress determined that the use of this information for employment, insurance and credit decisions was on balance good for society. The interest a person with negative credit has in concealing the information was outweighed by the advantages to society as a whole in having

[127] Federal Trade Commission, "In the Matter of BJ's Inc., a corporation," September 20, 2005 p. 3 at http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf. See also Beales and Muris assertion that harm need not be restricted to actual harm: "When intentional theft of information has occurred, the Commission need not prove actual fraud to prevail in an unfairness case, particularly if the interval between the breach and its detection is short enough that fraudulent use may not yet be observable." Beales and Muris p. 133

accurate information for crucial eligibility decisions.[128] The assessment of countervailing benefits has to be made at the social level.

The role of privacy externalities is relevant here as well. In examining whether an information practice has net benefits, all the consequences have to be assessed. This includes positive and negative consequences and internal (to the data subject) and external (to others) consequences. If revelation of information by some results in revelation of information about others, the consequences of this external effect, positive and negative, have to be considered.

The balancing test of whether the use of information has net benefits applies to secondary uses as well. The assessment of the possible benefits of secondary use of information is especially important. Even if some people might be hurt by secondary use, society as a whole might benefit. The assumption that all secondary uses of information are harmful is not sustainable. A demand that all data be destroyed after the initial use is accomplished is effectively a judgment that all secondary use is harmful. So is a requirement that data collectors return to the data subjects for affirmative consent before secondary use. For this reason, part of the European Privacy Directive is worrisome.[129] By putting an affirmative choice requirement on all secondary uses, these rules effectively make a substantive policy decision that these uses are not worthwhile and should be discouraged.

F. Does the FTC Have Authority to Use Unfairness in Privacy Cases?

When the FTC first began to consider privacy on the Internet, it invoked its deception authority rather than its unfairness authority. In a 1998 report to Congress it outlined what it perceived to be the limits of its authority in the privacy area:

> The federal government currently has limited authority over the collection and dissemination of personal data collected online. The Federal Trade Commission Act (the "FTC Act" or "Act") prohibits unfair and deceptive practices in and affecting commerce. The Act authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and provides a basis for government enforcement of certain fair information practices. For instance, failure to comply with stated information practices may constitute a deceptive practice in certain circumstances, and the Commission would have authority to pursue the remedies available under the Act

[128] The social decision to allow credit bureaus was not made under the FTC's unfairness authority, but directly by Congress. But it illustrates the point that the compensating benefit has to be social in character. The decision to allow full file credit bureaus is not the only possible decision. Other countries prefer do not allow credit bureaus or restrict them to negative information. See John Barron and Michael Staten, The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience 2000, available at http://www.privacyalliance.org/resources/staten.pdf

[129] European privacy requirements hold that information collected from a data subject should only be used for the specific purpose for which it was collected. Secondary use is permitted only with the affirmative consent of the data subject. See Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 Texas Law Review 553, 561 (1998)

> for such violations. Furthermore, in certain circumstances, information practices may be inherently deceptive or unfair, regardless of whether the entity has publicly adopted any fair information practice policies. As discussed above, Commission staff has issued an opinion letter addressing the possible unfairness inherent in collecting certain personal identifying information from children online and transferring it to third parties without obtaining *prior* parental consent. However, as a general matter, the Commission lacks authority to require firms to adopt information practice policies.[130]

The FTC repeated this point two years later in 2000, stating that it "lacks the authority to require firms to adopt information practice policies or to abide the fair information practice principles."[131] As a result of statements like this from the FTC and its practice of only bringing deception cases in the privacy area, many commentators concluded that the FTC could not use its unfairness authority to specify any particular fair information practices or to prohibit information practices as unfair.[132]

It is hard to understand the reason behind this. The FTC itself never explained why it thought it was limited in this way. One commentator tried to provide a reason:

> "The FTC's enabling act restricts its powers to situations where an unfair act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition…Due to the difficulty in monetizing many privacy violations and other problems in fulfilling this jurisdictional calculus, the FTC may face objections should it take an aggressive role in policing information privacy in cyberspace with no more authorization than the general grant found in its enabling statute."[133]

However, there is no requirement that the substantial injury test be monetized. As we have seen, it can accommodate real subjective preferences even if these preferences are not expressed in quantifiable terms, such as willingness to pay for products bought and sold in the marketplace.

As previously noted the FTC has taken steps to assert its unfairness jurisdiction in the area of information security. In the first case it brought it assert that "(BJs) failure to employ

---

[130] Privacy Online: A report to Congress June 1998 p. 41 at http://www.ftc.gov/reports/privacy3/conclu.shtm
[131] Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace." http://www.ftc.gov/reports/privacy2000/privacy2000.pdf under "Commission Recommendations."
[132] Daniel Solove, "In the end, however, the FTC is limited in its reach. It only ensures that companies keep their promises." The Digital Person, New York University Press, 2004, p.73; Paul Schwartz, Privacy and Democracy in Cyberspace, 52 Vand L. Rev.1609, 1638 (1999): "Web sites that make no promises about privacy…are likely to fall outside the FTC's jurisdiction."; Fred H. Cate, "the Commission was relying on its power to prohibit "deceptive" trade practices—i.e., practices that did not conform to published privacy policies—rather than its power to prohibit "unfair" trade practices." The Failure of Fair Information Practice Principles, p. 353.
[133] Schwartz Privacy and Democracy p. 1638

reasonable and appropriate security measures…was an unfair act or practice." [134] The harms in these cases included both monetized harms such as the financial losses to issuing banks and the less tangible losses of worry, inconvenience and time lost dealing with the problem. It is a reasonable extension of that practice to bring the FTC's unfairness authority to bear on larger privacy problems.

Several parties have explicitly called upon the FTC to exercise its unfairness authority in the privacy area.

> "The FTC should also continue to pursue enforcement actions and provide guidance to industry, but with a renewed emphasis and focus on a comprehensive set of Fair Information Practice Principles (FIPs). To do so, the FTC must reclaim its authority to fully enforce all of the FIPs under its unfairness jurisdiction." [135]

In light of the pressing need to move beyond disclosure, notice and choice and to evaluate directly the value of information collection and use practices, it would be important for the FTC to use its unfairness authority to examine whether certain types of information practices are harmful.[136]

A first step in that direction might be a survey of information uses in particular areas of concern such as online behavioral advertising, social networks and location privacy. In order for the public and policy makers to be able to assess an information practice it needs to be public. A comprehensive information policy might require an inventory of current and innovative uses of information. This could be supplemented with an ongoing survey of the new developments in information use. This would provide policy makers and the public with the background knowledge of industry practices they would need.

G. Related Models

The consequentialist approach recommended by former FTC officials Howard Beales and Tim Muris has affinities with the unfairness approach just outlined.[137] According to the consequentialist approach,

> "... the focus should be on the consequences of information use and misuse. There is little basis for concern among most consumers or policymakers about information sharing per se. There is legitimate concern, however, that some recipient of the information will use it to create adverse consequences for the consumer. Those consequences may involve

---

[134] Complaint, *In the Matter of BJ's Wholesale Club, Inc*, No C-4148, Sept 20, 2005 p. 3 available at http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf. Each subsequent case invoked the same unfairness authority.
[135] Refocusing the FTC's Role in Privacy Protection Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable, November 6, 2009 p. 4 available at http://www.ftc.gov/os/comments/privacyroundtable/544506-00026.pdf
[136] The FTC's unfairness authority can be used to ban practices, but it can also be used to impose other remedies such as disclosure.
[137] Beales and Muris

> physical harm, as when stalkers obtain information about their victims or child predators seek information online. They may be economic consequences, as when one's identity is stolen or when credit or insurance is denied based on incomplete or inaccurate information. Or there may be unwanted intrusions, such as the telemarketing call that disrupts the dinner hour or the spam that clogs our inboxes."[138]

This approach adopts the cost benefit test embodied in the FTC's unfairness standard. [139] They assert that there is an "absence of a privacy problem when consumers understand and have a choice about the information collection and use." In their harms-based approach, the role of choice is to legitimate an information use practice. Disclosure and the opportunity to refuse a service are all that is needed.

It is sometimes thought that the harm approach is restricted to tangible harms, but the Beales and Muris version does not contain that restriction:

> "I don't think there is anything in the harm-based approach to thinking about privacy that says we can only -- it can only deal with tangible harms. If you think about the very first case we brought under the consequences-based approach, it was a case against Eli Lilly that involved the release of e-mail addresses of Prozac users. A lot of them .gov addresses. And there's no tangible economic harm that goes with that as far as we know or knew or still know. There is a subjective preference on the part of many people that that kind of information shouldn't be out there and that, it seems to me, is what that case is about. Subjective values are important in a lot of places. They are important guides to what we do in the economy in products and services and privacy is no different about that. [140]

Beales and Muris apply the consequentialist approach largely to data security issues. The one example of the consequentialist approach relating to pure privacy had to do with the intrusions caused by telemarketing calls. But that decision was made under specific authority, not under the FTC's general unfairness authority. Beales and Muris do not extend the consequentialist thinking to other privacy examples, though the logic of their position leads to it.

The similarities between this consequentialist approach and the unfairness model are substantial. Both emphasize preventing harmful use. Both use a cost-benefit test. Both rely on the FTC's unfairness authority. Both would restrict choice when there are substantial public benefits at stake. Both allow for intangible harms. The main difference is that the Beales and

---

[138] Beales and Muris, p. 118

[139] "A far better approach to privacy protection is to focus on the consequences of information use and misuse for consumers. This approach directs attention to the relevant tradeoffs between benefits and costs of information use." Beales and Muris, p. 135

[140] Remarks of Howard Beales, p. 10 Exploring Privacy: An FTC Roundtable Discussion December 7, 2009, Panel 5 Exploring Existing Regulatory Frameworks at http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/120709_sess5.pdf

Muris consequentialist approach does not focus on the need to distinguish opt-in versus opt-out choice, and that it would allow even harmful uses of information if they had been subject to individual consent. The need to provide additional consumer protections beyond notice and choice is crucial for robust privacy policy, and is lacking in the Beales and Muris harms model.

The Business Forum for Consumer Privacy Center has developed a Use and Obligations privacy framework, which has affinities with the unfairness approach:

> But today, online and in public life, individuals, organizations and data analytics generate ever-growing amounts of data that fuel existing and emerging business processes. Wireless and mobile communications offer new points of data collection and provide new kinds of data. Open networks and the evolution of the Internet as a commercial medium and as a platform for connected services enable ubiquitous collection and global flow of data. Data about an individual can be easily copied and aggregated across vast, interconnected networks. That data, enhanced by analytics, yields insights and inferences about individuals based on data maintained in multiple databases scattered around the world. Asking the individual to assume responsibility for policing the use of data in this environment is no longer reasonable, nor does it provide a sufficient check against inappropriate and irresponsible data use in the marketplace.[141]

This approach focuses on use, not collection of information. It does not allow choice in certain circumstances including the use of information for internal business purposes, for fulfillment of services, for fraud and authentication services, and provides an opt-out for marketing uses. It recognizes that individual choice is not a sufficient test for protecting against harmful uses of data. It does not, however, call for the prohibition of certain data practices and does not embrace the use of the FTC's unfairness authority.

Daniel Weitzner and colleagues have developed an information accountability framework.[142] A key premise in this approach is that the "access restriction" perspective that has dominated privacy policy discussions must give way to an informational accountability and appropriate use model. The reason for this change is the development of ubiquitous data collection and growth of information analytics:

> In a world where information is ever more easily copied and aggregated, and where automated correlations and inferences across multiple databases can uncover information even when it has not been explicitly revealed, accountability must become a primary means by which society addresses issues of appropriate use.[143]

They reject the notice and choice model and embrace the idea that harm prevention and redress should be the goal:

---

[141] The Business Forum for Consumer Privacy "A Use and Obligations Approach to Protecting Privacy: A Discussion Document," Dec. 7, 2009, p. 2 http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf

[142] Weitzner

[143] Weitzner p. 1.

> Web users (could have) the ability to make privacy choices about every single request (for) collection (of) information about them. However, the number, frequency and specificity of those choices would be overwhelming especially if the choices must consider all possible future uses by the data collector and third parties. Consumers should not have to agree in advance to complex policies with unpredictable outcomes. Instead, they should be confident that there will be redress if they are harmed by improper use of the information they provide, and otherwise they should not have to think about this at all.[144]

The proposed solution to this situation is the construction tools that allow users of information to become aware of permissible uses and to limit their use in accordance with these constraints. While this framework is a start toward a new approach to privacy, it has not yet developed the specificity and the regulatory structure needed to be a replacement or supplement to the notice and choice model.

Fred Cate has proposed several Consumer Privacy Protection Principles for the regulation of harmful uses of information that is similar to the unfairness approach outlined here. He distinguishes per se harmful uses from per se not harmful uses. A per se harmful use such as the use of personal information to commit fraud is one which is always harmful. The government should prohibit these uses. Per se not harmful uses present no reasonable likelihood of harm. The government should not regulate those uses at all. Consent should be reserved for "sensitive" uses of information where the use is "reasonably and objectively thought to be intrusive, offensive, or otherwise invade personal privacy." The privacy protections should be subject to a cost-benefit balancing test, and the harms in question are tangible harms defined as damage to persons or property. [145]

The similarities are substantial, especially the overall division into uses that should not be subject to choice, those that cannot be allowed and those where choice is appropriate. He does not specify which agency of government would enforce these principles, but they could be carried out by the FTC using its unfairness authority with its cost benefit test. So his framework is consistent with the use of the FTC as an enforcement agency.

Some differences remain. His constraint that the harms have to be "tangible" harms that damage persons or property seems to be too narrow. His limitation of choice to those circumstances where there is a reasonable likelihood of harm seems too strong. The stronger test in the unfairness model for suspending choice is public benefit, where choice would prevent publicly beneficial uses. The unfairness model would allow for choice in substantially more cases. Finally, his model does not distinguish within the realm of choice between opt-in and opt-

[144] Weitzner pp. 1-2
[145] Cate Failure of fair information practices, p. 370

out corresponding to the relative closeness of an information practice to pure unfairness or public benefit use.

V. APPLICATIONS

The framework developed above can be applied to some of the cases discussed earlier. Invidious discrimination falls into the category of harmful uses of information. Information to be used for that purposed cannot be collected, even with individual choice, since choice allows information unraveling and adverse inference to be made about other people, thereby exposing them to invidious discrimination.

Scientific research on the other hand is overall beneficial and so should be allowed. The exception is the direct manipulation of an experimental subject that might expose him to significant risks. Here the IRB process provides for informed consent, supplemented with IRB review of experimental risks.

Data mining can be used for many purposes and its acceptability depends on the purpose. When information is used for price discrimination, access restrictions or inefficient product variety there is moderate to high risk of social harm. These practices are not per se harmful, but they create a significant possibility of external harms to people who cannot avoid the harms by individual consent. In these circumstances, it makes sense to raise the costs of collecting and analyzing the information used for these purposes as a way of controlling these extra risks. Requirements for notice and affirmative consent might accomplish this.

Use of credit bureau information for eligibility decisions is a social benefit. Since individual choice makes it impossible or extremely difficult for society to have this benefit, it makes sense to put these activities in the public benefit class where the default is that information will be shared and used for these purposes and no opt-out is allowed.

A. Online Behavioral Advertising

Online behavioral advertising involves the tracking of consumers' online activities in order to deliver tailored advertising. It usually involves three parties: a content provider who operates a website or other online service, an ad serving company, and an advertiser who wants to reach a targeted audience with a message. When a user arrives at a site, the content provider displays its material and sends a message to the ad server to fill in space on the site reserved for advertising. The information available to the ad server will determine what ad it provides to fill this space. This information can include information about the online activities of the visitor at that website, the activities of the visitor at other websites, personal sent by the content provider, and information from off-line data bases. By combining this information in various ways, the ad server creates a profile of the visitor and uses that profile to provide an ad that will be most

relevant to the visitor and most likely to induce him or her to click on the ad in pursuit of those interests.[146]

Online behavioral advertising involves the creation of a profile of the individual based in part upon his online behavior. Web-sites and ad serving networks place cookies (small bits of computer code) on visitor's computers that enable the website to recognize repeat visitors and tailor the web experience of the user based on prior visits and behavior at that site. Ad serving networks collect information based on visits to other websites and serve ads based inferences derived from these visits and other information. Both types of information profiling can be controlled through limitations on the use of cookies.

Online behavioral advertising is only a small part of the current online advertising market.[147] The economic advantage of targeted ads is that they increase the click rate. The advertiser will pay the content provider more for a targeted ad because more people click on it. The price of a contextual ad or a run of network online ad will be a fraction of the targeted return rate. For content providers, this creates additional economic support for their services.

One study estimates that targeted ads are 50% more effective in generating sales.[148] If so, that provides a way to estimate the economic damage that would result from regulation that reduced online behavioral advertising, either through the imposition of an opt-in notice and choice framework that was so unworkable it functioned as a ban or through the direct imposition of a ban. Take the example of online news sites. Currently, they generate approximately $3 billion in revenue for the newspaper industry.[149] Suppose the 50% figure is accurate. Then if all of this revenue is currently generated from targeted ads, then the regulatory elimination of targeted ads would imply a loss of $1 billion. If all of the $3 billion results from generic ads, then the elimination of online behavioral ads would block a potential gain of $1.5 billion, which is more than twice what could be reasonably expected from a pay wall strategy.[150] Any

---

[146] Edward Felton, Testimony before United States House of Representatives, Energy and Commerce Committee Subcommittee on Communications, Technology and the Internet, and Subcommittee on Commerce, Trade, and Consumer Protection Hearing on Behavioral Advertising: Industry Practices and Consumers' Expectations June 18, 2009. This describes how information needed for online behavioral advertising is collected and used.

[147] "Behavioral advertising as the industry usually talks about it, as a product, is a fairly narrow and specific category. And it's something like $1 billion today of the $23 billion of online advertising revenue." Comments of Berin Szoka at the Third Panel FTC Privacy Roundtable December 7, 2009, available at http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/120709_sess3.pdf

[148] Steve Lohr, Privacy Concerns Limit Online Ads, Study Says, New York Times, April 30, 2010 at http://bits.blogs.nytimes.com/2010/04/30/privacy-concerns-limit-online-ads-study-says/

[149] See Advertising Expenditures, Newspaper Association of America at http://www.naa.org/TrendsandNumbers/Advertising-Expenditures.aspx Online advertising was $3.2 billion in 2007, $3.1 billion in 2008 and $2.7 billion in 2009

[150] If the online world reproduces the 80-20 revenue split between advertising and subscription fee, then pay walls could generate only an extra 25% over and above the $3 billion level (or $750 million), even assuming that the pay walls did not reduce the online audience.

regulatory strategy, even one based on notice and choice, has to take into consideration the potential impact on worthwhile online content.[151]

Whatever the possible benefits, polls show that the public does not like the practice of online behavioral advertising. When asked 66% of respondents to a recent poll said they did not like it. The more they knew about the practice the less they liked it. When told how targeted ads were developed through the use of cookies, profiles and data analytics, the percentage of people disapproving rose to 84%.[152]

The current wave of public policy attention to online behavioral advertising arose in the context of the Google DoubleClick merger. In 2007, following the FTC approval of the combination, the agency held a workshop on behavioral advertising, followed shortly by a staff report containing recommended principles. After a public comment period, the FTC released a second staff report in February 2009 which contains the latest version of its guidelines for online behavioral advertising.[153] The issue of behavioral advertising was also a focus of its recent roundtable discussions of privacy.[154]

In response to the FTC's concerns, individual companies and trade associations have developed privacy principles and new tools to provide information to consumers to allow them to understand and control their experience with online behavioral advertising. Google, for instance, developed has a tool to provide users with additional transparency and control. Their Ad Preference Manager allows users to see what interest categories Google has assigned them, edit their categories or opt out entirely from receiving interest-based ads.[155] Yahoo has a similar tool called the Yahoo Ad Interest Manager.[156] The Network Advertising Initiative, an industry association of advertising networks, has developed a set of principles for notice, choice and

---

[151]These calculations are only illustrative so no real conclusions about regulatory policy can be drawn from them. The actual impact on newspapers might be substantially smaller. One commentator at the FTC's December 7 Privacy Roundtable suggested this in his comments on the increased effectiveness of behavioral advertising: "… if you look at increases in click through rates and the other metrics that are used to track the effectiveness of advertising, for the first year publisher, things like newspaper websites, the difference may be relatively small. It might be only twice as effective, twice as revenue producing. For small sites, it could be in many cases up to, again, a lot of data out there, but it could be up to ten times revenue producing." http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/120709_sess3.pdf

[152] Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessy, Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It, September 2009.

[153] Federal Trade Commission Staff Report on Self-Regulatory Principles For Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting & Technology February 2009. http://www.ftc.gov/opa/2009/02/behavad.shtm

[154] Federal Trade Commission, Exploring Privacy: A Roundtable Series http://www.ftc.gov/bcp/workshops/privacyroundtables/.

[155] Pablo Chavez, Comments in FTC's Third Privacy Roundtable, April 14, 2010 available at http://www.ftc.gov/os/comments/privacyroundtable/544506-00134.pdf. The program has produced some data for understanding consumer preferences in this area: "While our data is preliminary, we have noted that for every user that has opted out, about four change their interest categories and remain opted in, and about ten do nothing." Ibid, p. 4. The number of Google users actually going to this site to you it, however, is "small." See comments of Alan Davidson, Panel 3, Exploring Privacy: An FTC Roundtable Discussion (Dec. 7, 2009), http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/120709_sess2.pdf

[156] See Yahoo Ad Interest Manager at http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html. Like the Google tool, this software allows users to see, edit and opt out of the interest categories to which they have been assigned based on their web browsing history. It does not reveal the web-browsing history itself.

dispute resolution and a way for consumers to opt out of being tracked for the purpose of receiving targeted ads.[157] The Future of Privacy Forum has tested an icon that provides additional information about targeted ads. The initiative is designed to give "users control and transparency right from the advertisements themselves by featuring a behavioral ad icon and giving "clear notice" about the origins of targeted ads."[158]

These initiatives are designed to respond to the problems associated with unread privacy policies and to engage users with easy to use tools aimed at giving them more responsibility over their own data collection and use. They take the informed consent model to new levels of usability and convenience.

Despite this there are limits to what notice and consent in the area of online behavioral advertising can be expected to achieve. The basic problem is that it requires of users a level of technical competence and interest that is simply unreasonable to expect. For instance, many users know how to control the use of text cookies through instructions to their browsers not to accept third-party cookies or to delete cookies at the end of every session. The new tools will add transparency and additional granularity of control. But not many users know about the "flash cookies" that can be placed on their computers through the use of Adobe's Flash Player. These locally stored objects remain on a user's computer even after regular text cookies have been deleted and can be used for independent tracking or for restoring deleted text cookies.[159] Users can control the use of flash cookies through settings that are available at the Flash player website. Despite the fact that these cookies are found on approximately 98% of computers, few are aware of these settings or use them.[160]

Approached through the lens of notice and choice, the debate about privacy and online behavioral advertising will reduce to a discussion about the default. If an opt-in is required, then almost no one will opt in and the default will mean that online behavioral advertising will cease. Since policymakers do not want that result, the fall-back is an opt-out. Legislation such as the draft Boucher bill can require websites and ad serving networks to go through the steps of providing notice and opt out, but they cannot force users who have lots of things to do with their

---

[157] See http://www.networkadvertising.org/index.asp for a summary of these initiatives. This NAI opt-out regime relies on opt out cookies that a user can install on his computer. A technical problem arises with this regime. When users choose to delete cookies, for example by setting their web browser controls to delete cookies as the end of each session, this also deletes the opt-out cookies. Third-party software providers have developed a browser plug-in that remedies this problem at the end. See, for example, the Targeted Advertising Cookie Opt Out plug in available at https://addons.mozilla.org/en-US/firefox/addon/11073. Users who want to avoid tracking are advised to set their browser controls to reject third-party cookies or to delete cookies at the end of each session.

[158] See Future of Privacy Forum at http://www.futureofprivacy.org/2009/11/11/1565/ for a full discussion of their icon project.

[159] Ryan Singel, "You Deleted Your Cookies? Think Again," Wired, August 10, 2009 available at http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/

[160] See the privacy settings at the Flash player web site at http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager02.html#118539. In addition, browser plug-ins allow users to monitor and delete local shared objects. See, for example, BetterPrivacy 1.47.4 at https://addons.mozilla.org/en-US/firefox/addon/6623/

time to chase down the latest technology, learn enough about it and then determine what level of web tracking they want. This would mean that online advertising will be largely unregulated.

The draft Boucher bill attempts to resolve this dilemma by imposing an additional requirement: as a condition of being able to engage in ad serving without opt in consent, third-party advertising networks cannot share user information with anyone else.[161] But this requirement is too strong. It is effectively a judgment that no secondary services are worth it.

The FTC report touched on this key issue of secondary uses beyond online behavioral advertising. It noted that "some consumer groups cited potential harmful secondary uses, including selling personally identifiable behavioral data, linking click stream data to PII from other sources, or using behavioral data to make credit or insurance decisions." But it noted that "such uses do not appear to be well-documented" and therefore did "not propose to address this issue in the Principles at this time." FTC staff therefore decided to "seek more information on this issue and consider further revisions to the Principles as needed."[162]

This focus on secondary use is crucial. The profiles and segmentations constructed by ad networks for the purpose of serving targeted ads increase the efficiency of ad serving, but it is highly likely that these profiles will be used for other purposes. The investment in constructing these profiles will have a greater return when additional revenue from such secondary purposes is forthcoming. As with any information technology characterized by large scale economies, initial uses of the technology can help to defray all or most of the fixed costs of constructing the service. Additional uses of the technology can be had for marginal costs, which in these cases might be very small. This provides an economic incentive for offering these services at very low costs.

What might these secondary uses be? At the present time, very little is known about them. Using the unfairness framework described earlier can help to structure policy thinking about that issue. Where does the secondary Information use falls along the expected value continuum? For instance, the use of the behavioral ad profiles for racial discrimination is clearly a harmful use that should be prohibited outright. The use for scientific research, however, might be so important that it should be allowed regardless of the data subject's consent.

The biggest question is the use of the online behavioral profiles and analytics for eligibility and identification decisions. The benefits of using online profiles to aid employment, insurance and credit granting decisions are probably substantial. People's online activities, especially if subjected to various data mining techniques, will probably reveal highly predictive information for these purposes. Informational externalities are likely to be significant, both

[161] Draft Boucher bill p.
[162] Staff Report, p. 45

positively and negatively. The more people whose online activities are subject to these analytical techniques the more reliable will be the inferences that can be made from the data. The more predictive they are the more likely they will be to be used to evaluate people for eligibility decisions.

Do policy makers want to permit this? The basic reason for thinking clearly about the policy option of not permitting it is the possibility that people will reduce their use of the Internet dramatically in order to avoid generating information that can be used against them in employment, insurance and credit-granting contexts. This chilling effect might be so substantial that it would block much of the vibrancy and innovation that has characterized the Internet so far. Looked at a different way, deciding that people can do whatever they want on the Internet without fear that it will be recorded in a data base that can be used against them in these key contexts (and publicizing this fact!) will remove some of the reluctance that many currently have in engaging fully in online activity.

On the other hand, the advantages of using these profiles for these eligibility purposes might overwhelm the disadvantages of discouraging online activity. The use of these profiles and analytics for these eligibility purposes will likely subject the firms gathering and analyzing the data to the provisions of the Fair Credit Reporting Act. Policy makers who want to allow these additional uses might want to clarify the regulatory regime that would apply.

B. Social Networks

Privacy policy changes at major social networks like Facebook have generated substantial complaints, and calls for regulatory action. The most recent concerns stem from Facebook's introduction of new features:

> The first feature, instant personalization, allows certain partner sites to use data from a Facebook user's profile to customize their online experience. For example, if a Facebook user visits Pandora, an Internet radio website, instant personalization will allow Pandora to create a custom radio station for the user based on their likes and dislikes from their Facebook profile. The second new feature, social plugins, allows developers to place a Facebook widget on their website so that visitors can "Like" a page or post comments. These interests can then be shown on a Facebook user's news feed and users can see their friend's activity. Both of these new features users can opt not to use.[163]

[163] Daniel Castro, The right to privacy is not a Right to Facebook, ITIF April 30, 2010, at http://www.itif.org/publications/facebook-not-right. These developments have created substantial excitement in the technology community and have fueled talk of Facebook overtaking Google. See Farhad Manjoo, "Will all those "like" buttons make Facebook bigger than Google?" Slate, April 22, 2010 available at http://www.slate.com/id/2251646/ and Chris O'Brien, Sorry, Google, but Facebook is the Web's most important company now, Mercury News, April 29, 2010 available at http://www.mercurynews.com/ci_14970594?source=most_emailed&nclick_check=1

Concerned Senators wrote to the Federal Trade Commission asking the agency to impose new regulations. Consumer and privacy groups filed an additional complaint with the FTC, citing the inadequacies of the Facebook disclosures and consent mechanisms. The key policy proposals recommended by concerned Senators, however, are essentially better notice and choice. And the key debate is whether consumers should be allowed only an opt-out choice or whether the company should first get consumer consent before sharing any information. Senators and consumer groups want the FTC to mandate opt in; Facebook already provides opt out.[164]

This misses the main source of concern. The main issue is not control. Facebook users do need an effective opt-out in some circumstances and perhaps Facebook should be required to get affirmative express consent before getting personal information for certain uses. In the unfairness framework the kind of disclosure, notice and choice provided should depend on an assessment of what is being done with the information.

The real issue is further use of the profiles that Facebook is compiling on its members and the use that can be made of the inferences that can be drawn from these profiles. Several examples of these uses are worth looking at. The first is the study conducted by students in Boston that found it possible to predict the sexual orientation of a Facebook member by examining the sexual orientation of his friends. A person might not have revealed his sexual orientation in his Facebook profile, but his friends had revealed theirs. An analysis of friendship patterns on social networks revealed a high probability that people share their friends' sexual orientation.[165] As commentators have noted this strikes at the heart of the view that sees privacy as control over information.[166] It also illustrates in a striking way the power of information externalities where one person's decision to reveal information can simultaneously and unintentionally reveal information about others.

The question for policy is what can be done with this information. It is one thing for researchers to conduct such a study. It is another for the information to be published on the

[164] For these developments, see Letter to Marc Zuckerberg from Senators Schumer and others, Aril 27, 2010 (asserting that personal information of Facebook users "should remain private *unless* a user decides that he/she would like to make a connection and share this information with a community.") available at http://schumer.senate.gov/new_website/record.cfm?id=324226 and EPIC et al, Complaint in the Matter of Facebook , May 5, 2010 available at http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

[165] See Matthew Moore, Gay men 'can be identified by their Facebook friends' Telegraph.com, September 21, 2009 http://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html

[166] See Project 'Gaydar' Boston Globe, September 20, 2009 available at http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/?page=1. Quoting Hal Abelson: "That pulls the rug out from a whole policy and technology perspective that the point is to give you control over your information - because you don't have control over your information."

Internet or in a newspaper, or to be sold to the highest bidder for whatever purpose the buyer wants to use it for. A crucial privacy question for social networks is how to deal with the further use of this information.

It is tempting to think that the solution is further attempts at concealment. One way to do this might be to have a default of secrecy of friends. Under this approach, no one should know anyone else's friends, unless people explicitly reveal them. This applies to all members of the Facebook network and to application providers as well. But this throws out the baby with the bathwater. The networking advantages of platforms such as Facebook largely derive from openness and sharing of information about relationships. Imposing a default of no sharing is likely to limit innovation, growth and development of this promising new technology. Unless policymakers want to approach this issue with the blunt instrument of a mandated no sharing default, they will be forced to look carefully at problematic uses and decide what to do about them.

A further secondary use of Facebook information that raises problems is the ability of third parties to use Facebook information to create files and scores that are useful for eligibility decisions. The process is straightforward:

> "Social graphs allow credit issuers to know if you're connected to a community of great credit customers. Creditors can see if people in your network have accounts with them, and are free to look at how they are handling those accounts. The presumption is that if those in your network are responsible cardholders, there is a better chance you will be, too. So, if a bank is on the fence about whether to extend you credit, you may become eligible if those in your network are good credit customers.[167]

The basic technique used here is social media monitoring. It was originally designed to help companies and high profile individuals to monitor their reputation online. Companies, for example, would be given the chance to see what people were saying about them online. The same techniques can be used to develop predictive models about the individuals who are discussing the companies online.

The result is that data mining of online activities and activities, profiles and friend lists on social network sites can not only help predict what ads people might pay attention to. They can help predict "whether or not you're a worthwhile risk for a credit card or a loan…"[168] Some firms in the area suggest that they are simply helping banks and other institutions "target" customers.[169] But other institutions indicated that they were indeed using the social networking

[167] Erica Sandberg Social networking: Your key to easy credit?, Creditcards.com, January 13, 2010 available at http://www.creditcards.com/credit-card-news/social-networking-social-graphs-credit-1282.php

[168] Conley, Lucas, How Rapleaf is Data Mining Your Friend Lists to Predict Your Credit Risk, FastCompany, Nov. 16, 2009. http://www.fastcompany.com/blog/lucas-conley/advertising-branding-andmarketing/company-we-keep

[169] See Aleksandra Todorova Could Your Tweets Affect Your Credit? Smartmoney, January 26, 2010 available at http://www.smartmoney.com/Personal-Finance/Debt/Could-Your-Tweets-Really-Affect-Your-Credit/?page=all

information to make decisions on what offers to make and to evaluate the creditworthiness of applicants.[170]

As in the online behavioral advertising case, the issue is complicated by the presence of information externalities. One user might not reveal much about his finances during his online visits and interactions. But his interactions reveal who his contacts and friends are. His social network can be charted and mapped. Other people in that network might have revealed their financial information, either online or directly to a financial institution with which they have a relationship. One way or another information about the original data subject leaks, despite his best efforts to keep the information secret. If the information turns out to improve his chances of credit or employment, this might be to his advantage. If not, he has suffered an external information harm.

The informed consent model does not help policymakers with the puzzles posed by these examples of secondary use. Short of reducing dramatically the effectiveness and innovative potential of social networks, blanket sharing restrictions will not work. The key question is whether it is worth it to allow the information practice of using social network information for eligibility decisions, and if so under what conditions. The balance, as in the online behavioral advertising case, seems to be between restricting the use of social networking information for these eligibility decisions in order to preserve the sense of uninhibited and wide-open interchange, or permitting them under an appropriate regulatory framework. The likelihood is that FCRA would apply to these cases, but if policy makers want to permit these uses it would be useful to clarify the applicable regulatory regime.

VI. CONCLUSION

In contrast to the informed consent model of privacy policy, the unfairness model sketched in this paper calls for substantive evaluation of the uses of information when making privacy policy. The basis for this idea that substantive privacy policy is needed is that consumers cannot be expected to master the ways in which information can be collected and used. In particular, they cannot be expected to follow the myriad ways in which information leaks, the way information about some people can be used to make inferences about others.

Despite a growing awareness of the power of data analytics to enable powerful inferences, many sophisticated Internet users maintain that individual control can still be effective. As one commentator on a recent New York Times article on online behavioral advertising said:

> I just don't get why most Americans put up with this. It really is creepy. And it's actually fairly easy to opt out. Using Firefox with Adblock Plus, NoScript and a few other

[170] Ginny Mies, Skeptical Shopper: Can Your Online Life Ruin Your Credit, PC World, March 23, 2010, (Mies) available at http://www.pcworld.com/article/192207

> plugins, I don't see ads. I clear cookies (including Flash cookies) at exit. I use secure VPNs to anonymize my IP address, and disable geolocation. You could too.[171]

Part of the point of this article is that most people will not do any of those things. And they probably cannot be educated into doing them either. It is simply not reasonable to expect them to keep up with the latest technological ways of gathering information about them and making inferences from the data collected. It is unreasonable to expect ordinary consumers to become experts at hiding information from people who spend most of their working day trying to get at it.

The lesson of information externalities, moreover, is that even if they could be persuaded to do all these things, they will still be subject to indirect information leakages. As data aggregation continues, as linkages among different data sets more extensive and as data mining analytics become more effective, predictive inferences about people will become more accurate. People will be less able to protect the secrecy of their information through concealment. Indirect inferences based on data analytics will reveal these facts with an acceptable level of certainty that people do not wish to reveal.

As one consumer group put it, "Even the most information conscious, privacy-sensitive consumer cannot escape being profiled through careful information habits."[172]

These profiles and analytic inferences can be used for a variety of secondary purposes, including making employment, insurance and credit granting decisions about people. The fundamental privacy question policy makers are facing is whether that is a desirable future.

That is one reason why privacy policy is so hard. It is possible to approach this fundamental question indirectly through a question of how to structure choice about data collection – should it be opt-in or opt-out? But policy makers really do not know whether to provide a default of data collection and use or its opposite unless they make an evaluation of the use. It is this use-based privacy model that needs to be developed and moved forward into the public policy arena.

[171] Mies
[172] WPF comments, p. 2