# Open Privacy Standards

## Intro

The extent to which privacy is a fundamental human right has generated serious philosophical debate over the past few centuries. Three theoretical frameworks have emerged from these debates and are utilized in different ways by policymakers tackling information privacy issues: fair information practices principles, harms, and contextual integrity. All three are appealing, but ultimately the harms framework is the only one that can overcome the policymaking challenges facing lawmakers and government bureaucrats today.

The following aruges for the harms framework as a robust foundation for privacy using contemporary ideas of open government as a theoretical foundation. The first section argues that other frameworks, particulary the conventional Fair Information Practices Principles and the persuasive Contextual Integrity, are inadequate because of functional flaws that make them either myopic or overly rigid. The final section briefly outlines a mechanism revolving around the harms framework that involves small pieces of legislation directed at specific public policy outcomes. These bits of legislation and regulation come together to form open policymaking interfaces analogus to the application programming interface from computer programming.

## Philosophical foundations of the information privacy debate

While there is no shortage of philosophers writing on the subject, there are three whose works were particularly relevant to contemporary discussions of information privacy. The hard utilitarian view of Jeremy Bentham, the more tempered one of John Stuart Mill, and the Immanuel Kant's libertarianism have significant value to the conversation about privacy rights and policy in the information economy.

Jeremy Bentham's utilitarian view of privacy as one economic preference out of many informed his famous advocacy for the panopticon prison where the rights of the prisoners to go about their lives privately outweighed the value of a more efficient prison system. His solution was a prison system based on possibly constant surveillence. Bentham's brutal utilitarianism saw rights and laws as human creations, tools for evaluating the sum of total happiness in society. Privacy was not among those rights unless we decided to make it one. Government interference should be made to improve that sum.

Bentham stood in contrast to other philosophers like Immanuel Kant who took a friendlier view toward human rights and privacy in particular. Privacy, for Kant, was one among many rights that deserved protection. An individual's right to privacy was part and parcel of his or her human dignity. Invading privacy was akin to any other assualt that reduces one huamn over another. Kant struggled, however, to provide any mechanism for figuring out what was considered a right or not.

If Kant and Bentham were opposed, John Stuart Mill offered some middle ground. Mill was a utilitarian less focused on happienss as he was on progress of humankind. Progress, Mill argued, does not always make every individual or group happy, nor should it, but he also recognized that it *could* do harm. The government's job, then, was to intervene when societal progess turned into societal harm. Privacy was ultimately a good thing to protect because of the variance and experimentation it encouraged. Echoing Bentham's notion that privacy can affect an individual's behavior, Mill recognized that a lack of it could impinge an individual's ability to experiment with radical ideas and a lack of experimentation in society would ultimately harm it. Thus, privacy, while maybe not a right, was certainly worth protecting. For Mill, intrusions into individual privacy are done at the risk of inhibiting that individual's ability to contribute to society in meaningful ways.

Modern information privacy frameworks can be found in the penumbrae of these philosopher's ideas about personal privacy and the extent to which it should be protected. In each we see the influence of Kant's concern for individual rights and liberties, but we also see some notion of the utilitarian caution against overreaching regulation and progress.

## FIPPS: The Well-Intentioned Enumeration

In 1973 the Department of Health, Education, and Welfare called upon Congress to adopt a "Code of fair information practices" with five specific directions in which information should be handled. These have since become known as the Fair Information Practices Principles (FIPPs) of information privacy as they have replicated through the United STates and the world as standards for privacy policy (Cate, 2006). The five original principles were:

1. A database's existence should not be secret (transparency).
2. An individual should have some means of finding out what information about him or her is in a database (accessability).
3. Information collected for one purpose should not be used for another without the individual's consent (transparency).
4. A person should be able to amend information about him or her contained in the database (quality and correctability).
5. The organization or person who owns the database must assue the database's reliability (quality and security) (Cate, 2006).

These five were adopted into law by the Federal Privacy Act of 1974 to protect individuals from potentially harmful collection and use of information about them in federal databases. Eventually these basic concepts would, in some form, make their way into other US regulations (notably the FTC), the OECD the EU Data Protection Directive, and APEC's framework. Each agency adopting this framework has enumerated the exact language differently, some (the EU and OECD) more restrictive than others (the FTC), leading legal scholar Fred Cate to ask "which FIPPS" should we follow (Cate, 2006)?

Though Cate argues that FIPPs have entirely failed, they have done us some good. FIPPS works as a way of thinking about privacy and the values at stake when making public policy. The basic principle of transparency in data transactions speaks to a more deeply seeded value that there is a trust relationship in the disclosure of information between the one sending and the other receiving it. Similarly with the final principle, that information should be secure in storage. The desired public policy outcome is that in exchange for disclosing data to a third party, the individual will be given a fair idea of who has access to them, and for what ends.

The problem with FIPPs is that the mechanisms required to implement any kind of policy enforcing these principles is unwieldly. Instead of the desired public policy outcome, FIPPs-based policies result in meandering agreements, dozens of pages long written by corporate attorneys that individuals are supposed read before using the service. These jargon-laden policies almost always go un-read (fewer than 1% of users read privacy policies (Cate, 2006)). The opportunity cost for reading them is simply too high. McDonald and Cranor (2008)found the total cost to the American economy if everyone were to actually read the privacy policies of the websites they visit "on the order of $781 billion." What's more, that number did not include time to make an informed decision about whether to accept of reject the policy or compare it with other websites and services. If nobody is reading the statements to which they are agreeing, the FIPPs are not accomplishing their public policy goals. In fact, they may be doing more harm than good.

The Consumerist and many others recently reported a stunt carried out by GameStation wherein by agreeing to the terms of use, the UK-based online game retailer "owned the immortal souls" of its customers (Consumerist, 2010). While this is obviously a ruse and the terms of service is a separate legal agreement from the privacy policy, in this case 7500 people were harmed by a public policy mechanism that also relied on a long and complicated legal agreement consumers were supposed to read but did not (Sauro, 2011). It is not hard to imagine an organization doing something similar to the privacy policies nobody is reading.

## What's the Scenario?

Another flaw of FIPPS was seemingly answered by Helen Nissenbaum with her theory of contextual integrity (CI): there are some privacy problems for which none of the many-enumerated FIPPS apply. Consent, for example, is not required for credit monitoring companies to collect, aggregate and process data about consumers. If it were, the only people who would consent would be those with good credit and the system would break down. Nissenbaum argued that the right to privacy has different social norms attached to it depending on where it manifests itself. There is economic incentive to being forced into the system for society (fewer bad loans being issued) and to the individuals (potentially better rates and access to credit when it is needed). Our right to privacy is consistent with the expectations we have of other individuals in society.

The problem with this framework is when more than one set of social norms exists in a given context. The health care industry, for example, is regulated through the Healthcare Insurance Portability and Accountability Act (HIPAA) more so than websites dealing with health information. A website like [PatientsLikeMe](http://patientslikeme.com), unlike a clinic, is not subject to HIPAA despite that their users exchange information about their health. Both are venues for individuals to seek information, advice, and therapeutic treatment for chronic and terminal illnesses. In the doctor's office the individuals can rest assured that those handling their information will do so consistent with HIPAA regulations. Online the same people are only subject to a corporate privacy policy that expressly states its intentions to share sensitive medical information. Violating that agreement has no consequence other than (possible) banishment from the site. According to contextual integrity, we should apply the same policy to both.

Would Nissenbaum like us to repeal HIPAA to bring hospitals into compliance with Patients Like Me, or the other way around? The former would threaten to stability and integrity of the medical industry; the latter would take away a fundamental principle to the website: that sharing is open and free. Even if Nissenbaum were to cede that information shared in a doctor's office is a different context than information shared on a patient support webiste, CI still runs into difficulties. If they are different simply because one is online, what does that mean for electronic medical records, or Internet enabled video-conferencing with doctors? Under which context should those be subject? There is not a clear answer for this real public policy issue under the contextual integrity framework.

## The end of the grand undertaking

The most compelling idea we can derive from Nissenbaum is a more basic idea that one privacy solution may not fit every privacy problem. There is a desire in Congress and other policyaking bodies (noably the European Union) to make policy in grand undertakings. Since 1995, for example, the European Union has had one privacy policy regulating every electronic data use regardless of who used it or to what end. If the current debates are any indication, we will continue to have one policy to rule them all.

This is less true in United States where we have many separate laws for different privacy problems (HIPAA in healthcare and the Graham-Leach-Bliley Act in banking, for example), but one need not look further than the failure of these policies to know that a change is needed. Former Federal Trade Commission Director Tim Muris remarked on the failures of Graham-Leach-Bliley which he said killed "acres of trees…to produce a blizzard of barely comprehensible privacy notices" in the banking and financial services industry (Muris, 2001). These are exactly the same kind of notices that Cate highlighted five years later. "This is a statute only lawyers could love," Muris continued, "we can do better" (2001).

The problem is that Congress, still seeks one-to-many solutions for their problems. Muris hinted at this flaw in 2001. A lack of consensus over how to proceed along with the other related data collection practices and the lack of data about possible negative externalities from such legislation led him to the conclusion that it was "too soon to conclude that we can fashion workable legislation to accomplish the goals" of protecting online consumers. Moreover, there were existing laws that gave agencies like the FTC an immense, under-ultilized toolkit for privacy education, enforcement, rule modification, and prosecution. If we were to make new legislation, we should exhaust other options first, and have a clear idea of what it should do and how it should work.

## Start simple: do no harm

Where to start that investigation is a tricky proposition. The FIPPs are already failing, so starting there seems counterproductive. And Nissenbaum's framework is unpredictable, and seems fraught with potential to create conflicting and confusing policy. A third way forward is the harms framework introduced earlier, sometimes also called the economic framework (especially by Posner, 1978). The balance of this paper will argue the harms framework, when paired with an agile policymaking structure, is able to overcome its own shortcomings and serve as a better guide for privacy than either FIPPS or Contextual Integrity.

The harms framework traces its roots back to the personal privacy theories of John Stuart Mill. Mill believed privacy was an important thing to protect because it was what allowed individuals to experiment with new ideas, new ways of living and laws interfering with that right should be made only to prevent harm from befalling individuals (Mill, *Liberty*).

Mill was particularly concerned with the adverse affects of government intervention on progress, and this view has had incredible staying power. Judge Richard Posner took a similar view calling privacy an economic problem (as it was indeed an economic interest) in 1978 when he anticipated the continued importance of information to industry. The problem is that information based industries demand disclosure of private information.

## Patients Like Me: Where's the harm?

Take the PatientsLikeMe example introduced earlier. The website functions as a symptom, condition, and treatment research center for patients suffering from eleven different chronic or terminal conditions. Through the site, members enter "demographic information, logitudinal treatment, sympotoms, outcome data, and treatment evaluations," plus their unique condition including "treatment histories adn evaluations on thousands of medical products" (Frost, et al 2011). The question for the harms framework is, should we stop this because it violates patient privacy? For the contextual integrity framework that answer certainly seems to be an unsatisfying yes.

The harms framework can treat this site separate from its context in health care to ask, are the patients here helped or hurt by their disclosure? The evidence, has shown PatientsLikeMe users actually derive great benefits from the site about different therapies and comfort at different stages of their diseases ([Wicks et al 2010](http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2956230/)). Furthermore, specifically to the question of user shared data, Frost and Massagli ([2008](http://www.ncbi.nlm.nih.gov/pmc/articles/pmc2553248/)) found that the disclosure of personal data allowed patients to engage in a constructive dialog around and encouraged self-management of their conditions. These researchers concluded "desgin innovations that promote data-centered patient conversation" were needed (2008).

PatientsLikeMe itself does not hurt, but what about the anonymous, lurking about the site learning about all these patients and their conditions? Or the troll, interloping on the conversation to encourage perhaps risky behavior among the site participants? What happens when the database is breached and ends up public? These are all good questions, especially given how little information is required to identify someone online, and ones the harms framework can address them through an agile policymaking structure.

## Government as a Platform (GAAP), O'Riley

Jeff Jonas and Jim Harper (2010) outline some of the responsiblities governments face regarding data privacy in their "Open Government: The Privacy Imperative." Some see large databases providing tremendous insight but the average citizen sees "threatening privacy violations" (Jonas and Harper, 2010). But the public policy problem is broader than controlling uses of private data, it should also be about building a simple system to prevent harm.

### The Privacy Open Policymaking Interface

Tim O'Riley (2010) champions a concept called "Government As A Platform" (GAAP)wherein government exits alongside other successful technological platforms. O'Riley's model puts government first as the infrastructural provider for a society based on openness and interoperability.

O'Riley says the first step is to build "simple systems" and let it grow over time. Simple systems that work may evolve into complex systems that work. What we have in the current American privacy regime is a complex system that does not work, and working backward is much harder.

Imagine a hacker exploiting a backdoor PatientsLikeMe left in their servers.Perhaps they left the backdoor open because they did not know enough about cybersecurity to detect it; they are a small start-up with employees stretched thinly in the face of rapid growth, after all. There is currently only a weak system of torts to bring their users justice. Now imagine if there were an Open Data Privacy Platform authored by Congress giving PLM and their consumers ready-built tools for keeping their data private. If they do not at least adhere to these standards, they can be held accountable for data loss. Such a platform would lower the barrier to entry in the online marketplace and also give citizens a robust means of discovering what measures are in place to protect them, and what happens to their data once they transfer it.

In order for any of this to happen, Congress and the Federal government need to transition away from a mode of legislation based on doing as much as possible to one that does very little, very well, and thus has a very big impact. If they start with privacy, we will be better off as citizens, and as consumers.

## Sources

1. Fred Cate, "Failure of Fair Information Practice Principles", Chapter 13 in Winn, J.K. (Eds), Consumer Protection in the Age of the Information Economy, 2006, pp.343-369
2. Perton, Mark, "Read Fine Print Or GameStation May Own Your Soul", The Consumerist 2010 URL: http://consumerist.com/2010/04/16/read-fine-print-or-gamestation-may-own-your-soul/
3. Sauro, Jeff, "Do Users Read License Agreements?", 2011 URL: http://www.measuringusability.com/blog/eula.php
4. Nissenbaum, Helen, Privacy in Context, 2010, Stanford University Press.
5. Richard Posner, The Right of Privacy, 12 Georgia Law Review 393 (1978) pp.393 - 404
6. PatientsLikeMe, "Privacy". 2013. URL: http://patientslikeme.com/about/privacy
7. Mill, John Stuart, On Liberty, 1863
8. Kant, Immanuel, Groundwork for the Metaphysic of Morals, 1785
9. Bentham, Jeremy The Panopticon Writings. Ed. Miran Bozovic (London: Verso, 1995). p. 29-95 URL: http://cartome.org/panopticon2.htm Accessed: 2013-03-12
10. MacDonald and Cranor, 2008
11. Muris, Timothy, "Protecting Consumers' Privacy", 2001, Delivered at "The Privacy Conference 2001," Cleveland, OH. URL: http://www.ftc.gov/speeches/muris/privisp1002.shtm
12. Frost, Jeana; Okun, Sally; Vaughan, Timothy; Heywood, James; Wicks, Paul, "Patient-reported outcomes as a source of evidence in off-label prescribing: analysis of data from PatientsLikeMe", 2011, Journal of medical Internet research vol. 13 (1) p. e6
13. Wicks, Paul; Massagli, Michael; Frost, Jeana; Brownstein, Catherine; Okun, Sally et al., Sharing health data for better outcomes on PatientsLikeMe, 2010, Journal of medical Internet research vol. 12 (2) p. e19
14. Frost, Jeana H, and Massagli, Michael P, Social uses of personal health information within PatientsLikeMe, an online patient community: what can happen when patients have access to one another's data, 2008 Journal of medical Internet research vol. 10 (3) p. e15
15. Jonas, Jeff and Harper, Jim, "Open Government: The Privacy Imperative", in Ruma, Laurel and Steele, Julia eds., Open Government, 2010, O'Riley Media, Sebastopol, CA
16. O'Riley, Tim, "Government As A Platform", in Ruma Laurel and Steele, Julia eds., Open Government, 2010, O'Riley Media, Sebastopol, CA.