DRAFT
Privacy, Option Value, and Feedback

Wendy Seltzer
Yale Law School Information Society Project
wendy@seltzer.org

June 17, 2012

Abstract

We have confused intuitions about privacy in public. Sometimes, relying on a rationalist paradigm of secrecy, we say "if you don't want something published to the world, don't do it where others can see": don't post to Facebook, don't converse on the public streets. Yet other times, drawing upon experience in natural and constructed social environments, we find that we can have productive interactions in a context of relative, not absolute, privacy: privacy is not binary.

Over time, we have worked out privacy-preserving fixes in architecture, norms, and law: we build walls and windowshades; develop understandings of friendship, trust, and confidentiality; and protect some of these boundaries with the Fourth Amendment, statute, regulation, tort, and contract. The environment provides feedback mechanisms; we adapt to the disclosure problems we experience (individually or societally). We move conversations inside, scold or drop untrustworthy friends, rewrite statutes. Feedback lets us find the boundaries of private contexts and probe the thickness of their membranes.

Technological change throws our intuitions off when we don't see its privacy impact on a meaningful timescale. We get wrong, limited, or misleading feedback about the publicity of our actions and interactions online and offline. Even if we learn of the possibility of online profiling or constant location tracking, we fail to internalize this notice of publicity because it does not match our in-the-moment experience of semi-privacy. We thus end up with divergence between our *understanding* and our *experience* of privacy.

Prior scholarship has approached privacy in public from a few angles: It has identified various interests that fall under the heading of privacy: dignity, confidentiality, secrecy, presentation of self, harm; it has cataloged the legal responses, giving explanations of law's development and suggestions for its further adaptation. Scholars have theorized privacy, moving beyond the binary of "secret or not secret" to offer contextual and experiential gradients.[1] Often, this scholarship reviews specific problems and

[1]Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, (Stanford

situates them in larger context.[2] User studies and economic analysis have improved our understanding of the privacy experience, including the gap between expectations and reality.[3] Computer science and information theory help us quantify some of the elements we refer to as privacy.[4] Finally, design and systems-engineering literature suggest that feedback mechanisms play an important role in the usability and comprehensibility of individual objects and interfaces and in the ability of a system as a whole to reach stable equilibrium.[5]

This article aims to do three things:

1. Introduce a notion of privacy-feedback to bridge the gap between contextual privacy and the dominant secrecy paradigm. Privacy-feedback, through design and social interaction, enables individuals to gauge the publicity of their activities and to modulate their behavior in response.
2. Apply the tools of option value to explain the "harm" of technological and contextual breaches of privacy. The financial modeling of real options helps to describe and quantify the value of choice amid uncertainty. Even without knowing all the potential consequences of data misuse, or which ones will in fact come to pass, we can say that unconsented to data collection deprives the individual of options: to disclose on his or her own terms, and to act inconsistent with disclosed information.
3. Propose a broader framework for architectural regulation, in which technological feedback can enable individual self-regulation to serve as an alternative to command-and-control legal regulation. Feedback then provides a metric for evaluating proposed privacy fixes: does the fix help its users get meaningful feedback about the degree of privacy of their actions? Does it enable them to preserve disclosure options?

Finally, we see privacy-feedback take a larger systemic role. If technology and law fail to offer the choices necessary to protect privacy, we can give meta-feedback, changing the law to do better.

Law Books, 2009); Daniel J. Solove, 'A Taxonomy of Privacy', *154 U. Pa. L. Rev. 477* (2006); Julie E. Cohen, 'Examined lives: Informational privacy and the subject as object', *Stan. L. Rev.* 52 (1999).

[2]Paul Ohm, 'Broken promises of privacy: Responding to the surprising failure of anonymization', *57 UCLA L.Rev. 1701* (2010); Orin S. Kerr, 'The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution', *Mich. L. Rev.* 102 (2003); L. Lessig, 'The Architecture of Privacy', *Vand. J. Ent. L. & Prac.* 1 (1999); Jeffrey Rosen, *The unwanted gaze: The destruction of privacy in America*, (Vintage, 2001).

[3]Alessandro Acquisti and Jens Grossklags, 'Privacy and rationality in individual decision making', *Security & Privacy, IEEE*, 3 (2005):1; A.M. McDonald and L.F. Cranor, 'The cost of reading privacy policies', *ACM Transactions on Computer-Human Interaction*, 4 (2008):3; C. Jolls, C.R. Sunstein and R. Thaler, 'A behavioral approach to law and economics', *Stanford Law Review*, (1998); R.H. Thaler and C.R. Sunstein, *Nudge: Improving decisions about health, wealth, and happiness*, (Yale Univ Pr, 2008).

[4]James Gleick, *The information: A history, a theory, a flood*, (Pantheon, 2011); C.E. Shannon and W. Weaver, *The mathematical theory of communication*, (University of Illinois Press Urbana, 1962); Cynthia Dwork, 'Differential privacy', *Automata, languages and programming*, (2006).

[5]Donald A. Norman, *Emotional Design*, (Basic Books, 2004); J.W. Forrester, *Industrial dynamics*, (MIT Press Cambridge, MA, 1961); Charles Perrow, *Normal accidents: Living with high-risk technologies*, (Princeton University Press, 1984); H.A. Simon, *The sciences of the artificial*, (the MIT Press, 1996).

Contents

1 Puzzles

Privacy scholars and commentators are frequently puzzled by seeming contradictions in people's attitudes toward privacy and their online behavior.[6] We say we value privacy, yet we expose our lives in great detail on Facebook; we say our locations are sensitive information, yet we "check-in" with Foursquare and carry mobile location-tracking and -reporting devices almost everywhere (our cellphones). The settings we choose, to expose these details only to "friends," turn out to be full of holes, both technical and legal, that permit unexpected disclosure: employees are fired when bosses find uncomplimentary Facebook posts through "friends-of-friends"; location-tracking enables "please-rob-me"; #occupywallstreet protesters are identified with facial recognition derived from photos they themselves posted and tagged.[7]

1.1 Privacy in Public and Technology

When thefacebook.com first launched in 2004, the site was confined to Harvard College, bringing to a new medium the paper-backed "Facebook" circulated among the freshman class. Through it, students could browse the faces, and now, chat with classmates and find overlapping classes or interests, in the closed community of their college peers.

Facebook founder Mark Zuckerberg's ambitions didn't stop there. As he saw the site's popularity and sensed its potential reach, he rebuilt and opened it to wider audiences, first to students at a few other colleges, then successively to any college, .edu email address, workplace, and finally to the world at large, apologizing all the while for overstepping users' privacy.[8]

With each step, the network became more heterogeneous, but for a long time, its users

[6] string cite

[7] news refs

[8] Liz Gannes, *The Apologies of Zuckerberg: A Retrospective*, (AllThingsD, November 2011) ⟨URL: https://allthingsd.com/20111129/the-apologies-of-zuckerberg-a-retrospective/⟩.

had little reason to take notice of these changes. To each of them, the site looked like *their* collection of friends, the news, photos, and events from those with whom they chose to connect; invitations to connect from those who knew which identifiers to search; and a few advertisements scattered around the edges. In many respects Facebook looked and still looks like a transplanting of offline social relations.

Yet, when Facebook changes its privacy settings to "share" user information with more people, be they additional members of the public or advertisers seeking more targeted eyeballs, it is not only changing from the terms to which its users contractually agreed (albeit generally without reading), it is increasing the divergence between the site's visible practices and its underlying information flows. This lack of transparency weakens the feedback mechanisms by which users might understand and adjust their behavior to match the site's actual practices. Disclosures to the company are asymmetrical, not matched by reciprocal disclosure back to the end-user of what will be done with the data.[9]

In November 2009, Facebook changed its settings to make users share more information publicly by default, and reduced their options to keep classes of information confined to networks and unsearchable.[10] Like earlier changes, this prompted public outcry and the privacy skeptics' response, "If you wanted to keep it private, why did you put it online?" Yet Facebook is but one example of the new possibilities technology can offer and the challenges we face adapting them to our ends. Only recently has this behavior earned the social network an FTC consent decree.[11] [Add more recent updates here or below?]

[9] Contrast Goffman's discussion of situated conduct, "what individuals can experience of each other while mutually present." E. Goffman, *Behavior in public places: Notes on the social organization of gatherings*, (Free Press, 1966)

[10] Federal Trade Commission, *Complaint, In Re: Facebook, Inc.* November 2011 ⟨URL: http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf⟩.

[11] Ibid.

1.1.1 Facebook's Feedback Flaws

Users adapt to technology, too, even in their privacy-aware behavior, as danah boyd has shown. Studying young people's use of social networking tools, she finds they communicate with publics, plural, deliberately crafting messages to the audiences they see.[12] boyd finds that her subjects do not blindly transplant behaviors from offline to online, but learn what an online environment offers and use its constraints and possibilities in communication. Thus users of the early Friendster built "Fakesters" to serve as meeting nodes where the social network site offered none.[13] Contrary to the complaint that "kids today are exposing too much because they don't know what they're doing," boyd finds that even teenagers shape their practices to the online environments and build complex systems around the simple signaling mechanisms they are given (updating "relationship" settings, reordering "top friends").

boyd and Alice Marwick document teens' use of "social steganography:"[14] growing up immersed in the technology of social networks, and vaguely aware that those conversations may be overheard even if purportedly limited to a circle of friends (perhaps because of defects in friends' privacy settings, overlaps among conflicting circles of friends, or mandatory disclosure of passwords to parents), teenagers often use oblique, coded language to keep references private to their chosen circle. This requires more advance planning – akin to a pre-shared key in cryptography – but it's also an outgrowth of the slang kids used to keep teachers from overhearing conversations at the back of the classroom.[15]

But we can only adapt to what we know is happening. When teens were told that college recruiters and admissions offices might look at Facebook profiles for evidence of

[12] danah boyd. (2008). Taken Out of Context: American Teen Sociality in Networked Publics. PhD Dissertation. University of California-Berkeley, School of Information.

[13] danah boyd, "Friends, Friendsters, and MySpace Top 8: Writing Community Into Being on Social Network Sites." First Monday, 11 (12) (2006, December).

[14] boyd and Alice Marwick, '"Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies"', (2011).

[15] Ibid.

suitability, many high school students changed their profile names so as not to be found by network outsiders.[16] Their profiles were already connected to those of friends, so the identity switch did not disconnect them from the network.[17] This would give them only weak privacy protection – anyone determined to figure out who they were could likely map the network and its associated photographs, but it evinces intent and might be sufficient to keep these contexts separate (particularly if the admissions offices used a heuristic like "Google for the person's name" to identify the "public facet" of an applicant's persona.

Signals. Technology can give us cues to the public with which we are conversing, or it can hide those signals. Facebook shows a set of recently updated "friend" photos on each user's homepage when it wants to prompt us to write for that audience. "Send a note to ___," it urges, trying to use social ties to pull lapsed members back.[18] Yet Facebook rarely reminds us of the further nodes on the "friends of friends" network who will also have access to our posts. It cultivates the sense of intimacy and immediacy without reminding us of the reach and duration of its networked posts.[19] Thus boyd tells of a teen who was dismayed to learn that her mother was among the "friends of friends" who could view her profile, connected through an aunt the girl had 'friended.' Her information sphere was decontextualized.

Helen Nissenbaum describes privacy as "contextual integrity," saying we have established norms of "appropriate information flows" within contexts of activity, and sense a breach of privacy when information revealed in one context is disclosed or used in a manner inappropriate to that context.[20] Nissenbaum explains a concept of privacy that is not

[16]Sarah Maslin Nir, An Online Alias Keeps Colleges Off Their Trail, The New York Times, April 23, 2010, http://www.nytimes.com/2010/04/25/fashion/25Noticed.html

[17]Their identities would be easily discoverable from these networks, as anyone who's found Facebook or LinkedIn eerily accurate at predicting as-yet unconnected friends will recognize. It would be wrong for Facebook to "out" these students, however, or for admissions offices to attempt to pierce these veils.

[18]If you haven't signed in for a while, Facebook sends a reminder message, trying to tug with the photos of friends who are reportedly "missing you."

[19]Imagine if before each posting, Facebook were to show you some peripheral acquaintances who could see the update, or to ask "Will you want this message to be visible next year?"

[20]Helen Nissenbaum, Privacy as Contextual Integrity; Privacy in Context: Technology, Policy and the

dichotomous, public or private, but varied according to the circumstances and contextual expectations of those sharing information.

The sociological and philosophical literature suggests that we are not being hypocritical when we demand privacy in public, rather we are reacting to unexpected and unwanted changes in our information environments, and seeking an intermediate state between secret and world-readable.

1.1.2 Legal Feedback: *Olmstead* through *Katz*, Making Privacy Visible

Technological change can make the prior boundaries of private space visible, even as it erodes or enhances them. The famous start of privacy scholarship, Warren & Brandeis's 1890 "The Right to Privacy," responded to the then-new technology of photography, building a "right to be let alone" against the "[i]nstantaneous photographs and newspaper enterprise [that] have invaded the sacred precincts of private and domestic life."[21] What was implicit must now be claimed explicitly in the face of new technological granularity. Norms and rules are needed to fill newly opened gaps. [22]

The law's adaptation to technology can tell a story of feedback mechanisms in action– and of the time that feedback cycle may span. When the Supreme Court first encountered the telephone wiretap in 1928, the President did not yet have a phone on his desk, although traffickers in illegal liquor had found the technology. [23] The Court's majority put the the still-high-technology in a frame they understood–that of physical intrusion and trespass. Without trespass, the Court held, there was no "search" or "seizure" and therefore no need for a warrant. "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and

Integrity of Social Life (2010)

[21] S.D. Warren and L.D. Brandeis, 'The right to privacy', *Harvard law review*, 4 (1890):5.

[22] Compare the evolution of gap-filling default rules, as conditions around contracts change.

[23] See *Olmstead v. United States*, (277 U.S. 438, 1928); As with most new technologies, pornography was probably there too.

that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation."[24]

Feedback to *Olmstead* took time. The Court's ruling increased the vulnerability of telephonic communications to police snooping, but it also publicly exposed that lack of privacy. Criminals, judges, and the general public learned that their conversations were liable to be tapped. As the telephone itself became more widely used, the legal rule triggered responses. States passed wiretap acts, to protect by statute what the Constitution would not, and in 1934, Congress included anti-interception prohibitions in The Communications Act, section 605.[25]

Thus when Charles Katz came before the Court in 1967 to protest the wiretapping of his (illegal wagering) conversation from a public telephone booth, the times, technologies, and legal norms had all changed.[26] The telephone was part of everyday life, for personal and intimate communications as well as business of the lawful and unlawful type. As important, the public and the Justices themselves had experience through which they could view the technology. Asked again "[w]hether a public telephone booth is a constitutionally protected area," the Court "decline[d] to adopt this formulation." Telephone calls now demanded greater solicitude, even when conducted from the relative publicity of a glass-walled "public" phone booth. Justice Harlan's famous concurrence came to be the test for which the opinion stands, setting a "twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' " We shall see similar evolution in the Court's most recent technological privacy case, *United States v. Jones*.

---

[24]Ibid., p. 466.

[25]See Brandeis dissent, "Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him." 277 U.S. 438, 476

[26]*Katz v. United States*, (389 U.S. 347, 1967).

2 *Information* Privacy

Let us not forget that it is *information* we are protecting. Information theory gives us tools for evaluating the privacy impact of disclosure, the amount of knowledge a new disclosure provides.[27] "Information is uncertainty, surprise, difficulty, and entropy."[28]

More specifically, we can determine how much a new disclosure adds to the observer's background knowledge, which varies with both the new disclosure and the content of the background knowledge, what Cynthia Dwork terms "auxiliary information."[29][30] To understand the privacy impact of a disclosure, both intellectually and viscerally, one need to know both the content of a current disclosure and how it interacts with that which is already available.

Latanya Sweeney showed in 1997 that birthdate, year, and zip code were enough to identify individuals from "anonymized" medical records. Using public voter databases as keys, Sweeney was able to pinpoint individuals' records, including that of Massachusetts governor William F. Weld.[31] Dwork indicates that a database can provide information even about someone who is not included in it.[32] As Paul Ohm describes, this field of computer science research shows the "surprising failure of anonymization"[33]: we often fail to realize how little entropy there may be in a given information set, and thus how much can be revealed by the addition of a small amount of linking information.

Ohm brings these concepts and insights to legal scholarship. Drawing on the work of Sweeney, Dwork, and Narayan & Shmatikov's deanonymization of the Netflix prize

[27] Shannon and Weaver, *supra* note **??**.

[28] Gleick, *supra* note **??**.

[29] Dwork, *supra* note **??**.

[30] For example, answering my phone "Wendy Seltzer" gives less information to one who already knows that the number is my cell-phone, unlikely to be answered by anyone else; it gives more to the robo-dialer that doesn't even know whether its randomly chosen digits will reach a working number.

[31] L. Sweeney, 'Uniqueness of simple demographics in the US population', *LIDAP-WP4. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA* (2000).

[32] Dwork, *supra* note **??**.

[33] Ohm, *supra* note **??**.

dataset,[34] he argues that "anonymization" prophylactics fail to protect privacy, and law will instead have to take a more intrusive regulatory course, "squeezing and reducing the flow of information in society, even though in doing so they may need to sacrifice, at least a little, important counter values like innovation, free speech, and security."[35]

The EFF's Panopticlick project shows the impact of entropy reduction with a real-time experiment: visit the panopticlick.eff.org webpage from your standard web browser, and it will tell you how uniquely that browser configuration can be fingerprinted.[36] With each new characteristic–screen size, revision number, installed font list, etc.– you differentiate yourself from others; a combination of these factors can pinpoint many individuals. Over the course of the experiment 83.6% of the 470,161 users showed unique fingerprints[37] – fingerprints from which they could then be identified as repeat visitors to the panopticlick server's logs – and, were this not a privacy-preserving experiment, across other sites as well. Advertisers and online publishers can and do use the browser fingerprints to track users and tag the seemingly "anonymous" visitor with identifying data across visits. Even the Web-browsing individual who dutifully purges cookies and refuses site registrations is being tracked by IP address, browser fingerprint, web bugs, and behavioral profiles built from and "retargeted" to these identifiers.[38]

2.1 Privacy Harms

So, what's the problem? The definition of privacy's "harm" has posed serious challenge for privacy scholarship and litigation. Privacy harms appear either too abstract to be cognizable

[34] A. Narayanan and V. Shmatikov, 'Robust de-anonymization of large sparse datasets', in: *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, IEEE (2008).

[35] Ohm, *supra* note **??**, p. 1706.

[36] http://panopticlick.eff.org/

[37] Peter Eckersley, 'How unique is your web browser?' in: *Privacy Enhancing Technologies*, Springer (2010).

[38] See generally, The Wall Street Journal's excellent "What They Know" series, http://online.wsj.com/public/page/what-they-know-digital-privacy.html Julia Angwin, 'The Webs New Gold Mine: Your Secrets', *Wall Street Journal*, (2010) ⟨URL: http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html⟩

by the law, or too concrete and individualized for the general population to recognize their threat.

Abstract harms, such as loss of dignity or autonomy in the face of underspecified intrusion, strike lawmakers and courts as too amorphous, their potential sweep so broad they must be cabined before "privacy-protection" encumbers all manner of legitimate activity.[39]

By contrast, other harms are too concrete for us, as members of the public, to recognize as widespread problems. We do not see ourselves in the man tailed around the country on suspicion of drug trafficking, or the woman who is photographed in deshabille in the workplace.[40] Precisely because of their detail: the loss of insurance coverage because of misinterpretation of a genetic test; the loss of face by revelation of false lurid details, they are easily distinguished from the mundane, at both the societal and the individual level. (This situation isn't like that; that could never happen to me.) Instead, we push back against laws that would restrict us to protect *them*. Some of the most salient harms are notable precisely for their *ab*normality. And yet, as Kahneman illustrates time and again, we also overestimate our own uniqueness and mis-gauge statistical arguments.[41]

The diversity of potential harms and conceptions of harm can appear to pose a problem. Dan Solove's 17-item taxonomy feels haphazard,[42] while other accounts trade completeness for cohesion. But from another perspective, this diversity–uncertainty, and the preservation of options in the face of uncertainty–is privacy's core value. Information privacy is the option for each individual to disclose or conceal information as he or she chooses, to deploy information or to take action inconsistent with it. Privacy is late binding and just-in-time choice.

I suggest that information privacy attempts to model the *option* value of information disclosure, but typically fails to do so because individuals receive insufficient feedback

[39] failed cases alleging abstract harm
[40] example cases of highly individualized harm
[41] Daniel Kahneman, *Thinking, Fast and Slow*, (Farrar, Straus and Giroux, 2011).
[42] Solove, *supra* note **??**.

from the market. Individuals do not assess uncertainty correctly (a common failing, seen in the financial crisis as well as in other transaction situations). They have less information-processing capacity than their institutional counterparts. unequal information, unequal awareness of flows. They cannot aggregate information in the same way commercial information-processors can, without taking part in as many parallel transactions: the business sees many more business-to-individual transactions than any individual, and can also engage in bulk purchases of information on which to engage in further data-mining. Privacy should help us correct for the unequal bargaining power derived from these informational imbalances.

2.2 Option Value

Options theory can provide a mathematical representation – and theoretical explanation – of the expected value of information privacy, a current position with unsettled future choices.[43]

In financial markets, the option to buy a stock differs from the stock itself by deferring the decision, at some current cost.[44] An option represents the value of *choice*; it is the right, but not the obligation, to buy or sell at a future time for a price set now. Options matter in a world of risk and uncertainty.[45] "Real options" extends the analysis from financial assets to other types of investment.[46]

[43] Is the "expected value" of financial modeling related to the "expectation" of privacy that serves to measure our Fourth Amendment rights?

[44] If it cost $2 to buy a $10 call option, that option would be $3 "in the money" if the stock rose to $15, and a loss of only $2 if the stock price fell to $5. Options thus provide opportunities for speculation, hedging, and arbitrage. See J. Hull, *Options, futures and other derivatives*, (Pearson Prentice Hall, 2009); C.Y. Baldwin and K.B. Clark, *Design rules: The power of modularity*, Volume 1, (The MIT Press, 2000) At times, of course, the leveraging features can wreak havoc in financial markets, and mathematical models can provide a false sense of certainty. Tim Harford, 'One maths formula and the financial crash', *BBC*, April (2012) ⟨URL: http://www.bbc.co.uk/news/magazine-17866646⟩

[45] As distinct from risk or probability, we take uncertainty to refer to the unmeasurable. See F.H. Knight, *Risk, Uncertainty and Profit*, (University of Chicago Press, 1921), and N.N. Taleb, *The black swan: The impact of the highly improbable*, (Random House Inc, 2007)

[46] A.K. Dixit and R.S. Pindyck, *Investment under uncertainty*, (Princeton University Press, 1994).

As distinct from simple net present value calculations, real options analysis accounts for irreversibility, uncertainty, and timing of investment decisions.[47][48] Moreover, a complex decision contains a set of embedded options, including the option to proceed, expand, or abandon now or in the future.

"a firm with an opportunity to invest is holding an 'option' analogous to a financial call option – it has the right but tnot the obligation to buy an asset at some future time of tis choosing. When a firm makes an irreversible investment expenditure, it exercise, or 'kills' its option to invest. It fives up the possibility of wating for new information to arrive that may affect the desirability or timeing of the expenditre; it cannot disinvest should market conditions change adversely."[49]

Information may be disclosed too cheaply if its embedded options are not accounted for. In purely economic terms, having options is better than not having them at the same price point. More options are better than fewer, yet here the cognitive load may conflict with the model. While a portfolio of options is worth more than an option on a portfolio, the human brain confronting the "paradox of choice" may cause us to throw up our hands.[50]

[47] Ibid.

[48] M. Schulmerich, *Real options valuation: the importance of interest rate modelling in theory and practice*, (Springer Verlag, 2010) Amram and Kulatilaka developed a list of criteria that show under which circumstances the real options approach is fruitful.

- 1. When there is a contingent investment decision.
- 2. When uncertainty is large enough that it is sensible to *wait for more information,* avoiding regret for irreversible investment.
- 3. When the value seems to be captured in possibilities for future growth options rather than current cash flow.
- 4. When uncertainty is large enough to make *flexibility* a consideration.
- 5. When there will be project updates and mid-course strategy corrections.

[49] Dixit and Pindyck, *supra* note **??**, p. 6.

[50] Barry Schwartz, *The Paradox of Choice: Why More Is Less*, 1st edition. (Ecco, December 2003), ISBN 0060005688.

2.3 Degrees of Freedom

Privacy's option portfolio is built from a set of components: the option to conceal or disclose information, and the timing of that disclosure; the option to act consistently or inconsistently with that information. Each of these options can be exercised by choice. Thus friends share secrets to seal a bond of trust;[51] a would-be business partner shares market information to show his value, but only after gaining some confidence that a deal is possible.

These options are lost when privacy is invaded: the option to conceal or disclose at a later date is taken from us by surreptitious surveillance or tracking. The options for future action can be limited by third-parties' action based on such tracking: whether it's steered through behaviorally-targeted advertising or opportunities foreclosed by a bad reputation among those privy to a social network. Disclosure of information constrains the data subject's future options; privacy protects those options, providing degrees of freedom in both dislosure and action.

Privacy also gives the individual information subject the benefit of uncertainty and unforeseeability. We cannot exercise choice without considering external constraints. Yet in many cases, we may be unaware of those constraints. What looks innocuous today may be revealing tomorrow. What if disclosing your distaste for coriander gives clues to genetic propensity to disease? Or, as OKCupid finds, that answers to "do you like the taste of beer?" correlate with those to "are you willing to have sex on a first date?"[52]) Is it "consent" when an individual answers the more innocent question and is judged on the more revealing?[53] Arguably, the validity of that consent is tempered by the amount the individual knows about how information may be used. But some correlations are discovered only after significant research, or become known only through later aggregation. May consent be vitiated by later-developed uses? or is a stronger consent to as-yet-undiscovered uses

[51] Charles Fried, 'Privacy', *Yale Law Journal* (1968), Berkman Kids and Social Media event, teens describing password-sharing.

[52] See http://blog.okcupid.com/index.php/the-best-questions-for-first-dates/

[53] I leave for the readers which of OKCupid's questions is the more sensitive.

possible. Amy McGuire denominates this problem that of "consent to uncertainty."[54]

Decisions about information disclosure are always made in the face of uncertainty about future interests. Technological innovation adds a new set of uncertainties, changing the scope of what can be done with existing information, the future value of past disclosures. Disclosure's value may decay over time as information goes stale[55], or it may increase with additional linkability and external info.[56]

We are also uncertain how information might be useful in the future. These new links and uses might be a second-degree source of uncertainty or unforeseeability: after-discovered information and after-discovered uses of information. Technology increases our capacity to store, aggregate, and draw statistical conclusions from information.[57] Once facial recognition is developed, it can tag not only newly-posted photographs, but also those posted years earlier. Compare the dejanews posting of Usenet archives: what was temporary and ephemeral became permanently public. Dejanews (and later Google) developed protocols for removing material from the archives to deal with this discomfort, but during the transition phase, many felt their privacy had been invated.

What would privacy derivatives look like?

2.4 Economics of Privacy

Option value gives another way of conceiving the value of privacy. Privacy is not just protection against embarrassing details, but the value of choice denied. Yet one might ask why that choice-value inheres in the individual. Following Coase into a transaction-cost-free world, wouldn't we be indifferent to who starts with the entitlement? Moreover, where transaction costs would make it difficult for an aggregator who could make more efficient

[54] Amy McGuire, cited in *"Here Is a Human Being: At the Dawn of Personal Genomics"*, (HarperCollins, 2010), p. 162 discussing how little we currently know about what genome sequencing may reveal.

[55] Narayanan

[56] Dwork, *supra* note **??**; Ohm, *supra* note **??**.

[57] Charles Duhigg, *The Power of Habit: Why We Do What We Do in Life and Business*, (Random House, February 2012), ISBN 1400069289.

use of information (to help shape individuals' choices, through price discrimination, or to guide product development) to gain it from its component-holders, shouldn't we put it with the aggregator and let individuals who value privacy more highly bargain it back?

The economics of privacy, however, owe more to Arrow and Hayek than to Coase. Information privacy preferences, or meta-information about the information we're willing to disclose, is an information good subject to Arrow's information paradox.[58] Because the information itself is both subject and condition of the market, we can't construct a functioning market in privacy information without first setting ground rules that permit individuals to retain control even once they've partially disclosed it.[59] Thus privacy is a necessary default to enable individuals to make local choices about information disclosure.[60] The preference information is "sticky," costly for the individual to transfer.[61] In the individual's hands, it's an option, in the aggregator's hands, the choice has been made.

Information intermediaries, trusted third parties, or "infomediaries" are often proposed to serve as go-between negotiators.[62] Yet none of these has succeeded so far as a *privacy* intermediary, and so long as the individuals are denied any rights, there's little incentive for the collectors to bargain with anyone. My argument is not of market failure so much as

[58]Kenneth Arrow, *Economic welfare and the allocation of resources for invention*, 1962: "There is a fundamental paradox in the determination of demand for information: its value for the purchaser is not known until he knows the information, but then he has in effect acquired it without cost."

[59]Arrow's information paradox is invoked frequently in intellectual property: that the market for information goods can't operate without protection because otherwise an attempt to show one's wares to potential buyers would end up showing the goods, whether the buyer paid or not. IP says that those who see but don't pay are forbidden from use.

Privacy does not operate in precisely the same way. People are asking for protection of their right to disclose/withhold, and seeking the help of intermediaries to do that. But some of them want to sell the information itself, at the right price; they can't know what their information is worth until they disclose it, either individually or as part of an aggregate? or they could read an actuarial table, but that would cause the purchaser to disbelieve the signal being sent. who wouldn't want to sell the most valuable info, rather than owning up to a less valuable status, unless it would cost him more? While the market for privacy is conceptually distinct from a market for private information, yet those identifying as wanting most privacy are also often revealing something about themselves.

[60]F.A. Hayek, 'The use of knowledge in society', *The American Economic Review*, 35 (1945):4.

[61]Eric von Hippel, '"Sticky Information" and the Locus of Problem Solving: Implications for Innovation.' *Management Science* (1994).

[62]See Clippinger, P3P, Certificate Authorities, Peppet draft

market incompatibility.[63]

2.4.1 The Value of Option Value

It might be objected that option value would over-assess the harm of potential disclosure. This should not be the case. The components of the option's valuation depend on both harm and likelihood – a harmful but unlikely event is discounted for its rarity; common but harmless events are counted at their minimal level of harm. (Do we assume risk-neutrality?)

A subjective assessment might not seem to get us any further than the prior determinations of harm. Perhaps by valuing a basket of potential outcomes we reach similar enough probability-weighted valuations that a mean is representative. This is similar to Paul Ohm's suggestion that we each have an entry in the "database of ruin"[64]–it may not be the same item for each of us, disclosure of which would cause serious harm, but so long as we each have items of similar weight, we can assert that the option value of the overall disclosure choice, lost to unchosen surveillance, is similar.

As compared to other measures of privacy, option value is more easily quantified than "dignity" or "autonomy," although it bears them some resemblance. It can value the diversity of privacy concerns in a uniform framework. On the other hand, the options themselves still have to reflect meaningful choice: multiplying a bunch of worthless options still leaves the holder with nothing.

Moreover, while this framework is meant to help match privacy protections to our intuitions about information values, humans have notoriously bad intuition around probability and statistics (as the behavioral economics literature highlights in its myriad deviations from "rational" actions).[65] We look to systematic feedback mechanisms to improve these

[63] Scott R. Peppet, 'Unraveling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future', *Northwestern U. L.Rev.* (2011), p. 4n16.

[64] Ohm, *supra* note **??**.

[65] A. Tversky and D. Kahneman, 'Judgment under uncertainty: Heuristics and biases', *Science*, 185 (1974):4157.

intuitions.

Challenge of aggregation: dribbling out of information is simultaneously less salient to us in the course of disclosure, and more revealing to the aggregators against a course of background knowledge.

2.4.2 Big Data versus Small Individuals

Privacy is plagued with information asymmetries. Individuals' information about their own privacy preferences is sticky to them. And on the other side, its value to aggregators of "big data" derives from the aggregation, and secondarily, often, from the inferences that aggregation allows them to derive about the data subjects (and others outside the data-set).[66] Each party has different knowledge of information's value and different values for it.

Power/information imbalance when marketers know more about the subject population than its members do. Market-power enhancement, when the aggregators get richer - additional information has more value to Google, who already has lots, than to little guy. We don't have an intuitive sense of this imbalance. Privacy relates to power; there have always been those with the power to look further/deeper than you, against whom we depend on law to protect. David Brin proposed that technology would give us sousveillance, the opportunity to watch the watchers,[67] but that response is incomplete so long as the powerful can continue to override *their* watchers.

2.4.3 Network Effects

Network effects and lock-in are a challenge to in-market attempts to push back. Social networking technologies are classic network effects businesses. Their value to us depends

[66] See *Dwyer v. American Express*, (652 N.E.2d 1351 (Ill. App. 1995), 1995), in which the plaintiffs' case against aggregation of credit card history and personalized targeting based upon past purchases foundered on failure to show individualized "harm."

[67] David Brin, *The Transparent Society: Will Technology Force Us To Choose Between Privacy And Freedom?* (Basic Books, June 1998), ISBN 0738201448.

largely on the extent to which they're adopted by the peers with whom we want to interact – even if we want to interact only with small numbers of them and do not want to become the next @aplusk with millions of "followers." If those particular people with whom we want to interact aren't there, it's much less useful; while if they are, we may stick with it even if we dislike its practices, because the switching cost of moving all of our friends along with us is too high. (Interesting privacy dilemma: we'd be able to move our friends list more easily if we didn't demand privacy of our social connections-list,[68] but that's not the only barrier because some services claim it's *their* property too!)

2.5 Context and Attention Span

Social software induces context-errors: information given in one expected context is showing up in another. As Helen Nissenbaum describes, our expectations of privacy are often contextual; we mean for different things to happen when we talk about an illness with a friend and with a doctor.[69]

The market is unlikely to give us perfect (or even sufficient) context control, in part because breaches of context can help us enough that we choose them at times. A new social network service that comes pre-populated with a list of our friends will fail if it gets those "friends" wrong;[70] but may succeed if it uses those guesses to guide our perception of an attractive environment and lower our barriers to using it productively.

[68] Ben Laurie, 'Why Privacy Will Always Lose', *Links* (2009).

[69] See Nissenbaum, Privacy in Context (2010).

Contexts can be like classes in an object-oriented programming environment. Calling the same method in a different class will give behaviors that have a family resemblance, but vary in their particulars. So "print" will generally do something sensible, while inheriting specifics from its class context, such as format for display or for paper. As in object-oriented programming, context-switching has an overhead, but in complex environments, it can be less than that of building expectations from scratch on each encounter. It's a heuristic. Even among friends, you can override the default expectations of information sharing by saying "I want you to keep this secret," often with a from X or because Y. ("This is a surprise party" builds one subcontext; "I'm afraid it will get me fired" builds a different one.

[70] See Google Buzz; Christian Crumlish and Erin Malone, *Designing Social Interfaces: Principles, Patterns, and Practice s for Improving the User Experience*, (O'Reilly Media, Inc., September 2009), ISBN 9780596154929, p. 375 (describing the "ex-boyfriend" anti-pattern).

Errors are so common here that critics have noted the "uncanny valley" problem: as something too photorealistic in computer-animation immediately impresses on us all the little details that fail to match, while something that's more obviously artifice – less detailed – can trick us into filling the gaps ourselves, and thus finding it more "real." Artificial social networks can either delight us with the clever suggestions they offer, or perturb us with the bugs among the correct answers. Networks that control less are more generative, operate as scaffolding for us to fill in our own detail, and use in unexpected ways, perhaps as modules in our own creations.[71]

Privacy in context connects up with the "attention span" problem. Jeffrey Rosen and Lawrence Lessig both posit privacy as a solution to the short public attention span. When we learn a few embarrassing facts about a person out of context, we may base our judgment of him on those facts – which fail to capture all of the person and likely misrepresent him. Privacy serves to keep those facts out of casual view, until they can be seen in the context of the larger personal history and justification. Lessig thus describes how an email written in haste to an acquaintance at Netscape was drawn, from the public record of the Microsoft antitrust suit (in which Microsoft challenged Lessig's appointment as special master), into erroneous assumption of personal bias, mistaken reporting on the reasons for his disqualification (jurisdictional), and even misguided speculation about his sexual life.

Rosen writes at length about public figures drawn into allegations of sexual impropriety: Clarence Thomas, Bill Clinton, and Monica Lewinsky among them. Each was turned for a time into a caricature, known primarily for these allegations. Rosen calls the effect "synecdoche," from the literary figure in which a part stands for the whole.[72] Prurient details in particular tend to capture public attention.[73] Where the person has other claims to the public's attention, such as Clinton as the presidency continued post-impeachment, he

[71] There's a dilemma, though, in that the greater modular composability a socnet provides, the less context it can assure.

[72] Jeffrey Rosen, The Unwanted Gaze, 138.

[73] See also Strahilevitz, Privacy and Social Network Theory.

may be able to rehabilitate himself. Yet Monica Lewinsky has almost no chance of escaping her label "intern in the blue dress" and Justice Thomas remains, to many, the joke of the pubic hair and the Coke can.

The cases of Clinton and Thomas illustrate an "aspect of the phenomenon of the synechdoche: those with unlimited access to the public's attention have a greater chance of being judged in context than those who do not," Rosen says.[74] Since most of us are not public figures on the scale even of Clarence Thomas, we face his risks.

Now, it may be true, as Lior Strahilevitz suggests, that most of us overestimate our centrality in social networks and believe too readily that our friends will grasp at our every embarrassment. He recognizes the danger to over-correcting our perceptions of the publicity of our actions.. "The danger, at least from a privacy perspective, is that people learn to stop being surprised by these encounters, and guard their personal information too much as a consequence."[75] But unless we find ways to recalibrate our inner censors, this suggests that if given accurate, transparent reporting of what technology knows about us, we will clam up too much, and fail to share information in contexts of friendship and intimacy.[76]

Finally, the peccadilloes of public figures are part of feedback mechanisms about privacy-failures. Congressman Anthony Weiner misjudged his audience or potential audience when sending private messages on Twitter.[77] But he also misjudged the privacy settings as a social matter: even if he set all the right "privacy settings" through technical interfaces, he couldn't prevent one of a private message's recipients from forwarding it on, saving, or disclosing it. For a public figure, there may be more risks that someone will break the context, as the pressures . Was he confused audience misjudgment, persistence of messages. these examples help educate the broader public about the limited privacy they should in

[74]Rosen, The Unwanted Gaze, 157.

[75]Lior Strahilevitz, *A Social Network Theory of Privacy.* (2004).

[76]fried68

[77]'A Weinergate timeline', *Salon*, (2011) ⟨URL: http://www.salon.com/2011/06/01/weinergate_timeline/⟩.

fact expect.

3 Feedback

Here, we introduce a notion of privacy-feedback to bridge the gap between contextual privacy and the privacy-as-secrecy paradigm. Feedback shows us and those with whom we interact the scope of the contextual membrane around our interactions. It reflects to us how actions and disclosures will be perceived, ideally at a time that helps us to make current and future decisions. [[The more feedback is delayed, the more challenging it will be to correlate cause and effect, and to give the feedback salience in decision-making.]]

3.1 Three information pathways: governments, corporations, and peers

Individual privacy is nonetheless always a relational concept. The "right to be let alone"[78] takes its valence from the context of interactions with others. It's not meaningful to speak (only) of the hermit's privacy, or to demand that we all become hermits if we want to reclaim privacy. Rather, we must speak of controls over the disclosures that we make living in society, of information that is partially shared.[79]

Privacy thus relates to links, relations, contexts,[80] to our place in another's attention.[81] Our experience of privacy is only partially within our control; the rest depends on the discretion of those with whom we interact. We may have in mind different indirect objects of the "privacy from," namely, from the government; from corporations, as service providers, proprietors of networks, and vendors; and from other individuals (what Jonathan Zittrain labels "peer-to-peer" privacy).[82]

Although they are also private actors, corporations differ from peers in their scale and

[78] Warren and Brandeis, *supra* note **??**.

[79] See danah boyd, http://www.zephoria.org/thoughts/archives/2011/11/20/debating-privacy-in-a-networked-world-for-the-wsj.html "[P]rivacy is not simply the control of information. Rather, privacy is the ability to assert control over a social situation."; Solove, *supra* note **??** citing Barrington Moore

[80] Nissenbaum, *supra* note **??**.

[81] Rosen, *supra* note **??**; Lessig, *supra* note **??**.

[82] Jonathan L. Zittrain, *The Future of the Internet–And How to Stop It*, (Yale Univ Pr, 2009).

over large parts of our communications infrastructure (as intermediaries (ISPs, payment providers), as proprietors of key network meeting-points (Google, Facebook), or as advertisers with tentacles in many places. The government has coercive power over us and over the others in our network: it can obtain information from corporate keepers with a subpoena under the "third party doctrine," from our peers by enlisting them as informants, and from us or our homes with a warrant; increasingly, it also obtains information by surveillance, arguing that this is not "search" or "seizure" and thus requires no warrant.[83]

While the rules and norms by which information is obtained will naturally differ for differently situated actors, they should vary less widely than they do. We set our expectations of privacy parsimoniously, based on the most common interactions, with our peers. Since our encounters with peers are more frequent and offer more rapid feedback than those with companies or government, we shape our privacy expectations by them. If the information available to government or companies is different or greater, it's hard to adjust our expectations and behavior. Unless given much more explicit warning about the variance, – and opportunities to correct our behavior, we'll be unpleasantly surprised by the uses others want to make. Moreover, we don't want to have to interact with our friends only on terms we'd want corporations and the government to know.

3.2 Social Feedback

As described above, our expectations of privacy are built on social experience. Incomplete as these pictures of reality may be, reading the signals others send and their reactions to ours teaches us to modulate our own behaviors.[84] We make inferences based on limited information ("they're holding hands, they might be in a relationship"; "she's dressed in a business suit, she's headed to a job (or, in Silicon Valley, more likely a job interview)".

[83] Although its most recent high-profile effort to do so was rebuffed by the Supreme Court in *United States v. Jones*, (http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf, 2012)

[84] J. Donath, 'Signals in social supernets', *Journal of Computer-Mediated Communication*, 13 (2007):1.

We learn these cues from seeing them in others, and watching as they are validated or invalidated. Sometimes, we find our inferences are wrong and correct our perceptions and the signals we send to others. Moreover, we can develop relatively sophisticated social understanding of cues, learning to recognize when our perceptions are outside the norm, as well as when our behaviors are. [85] As children, we learn to mirror the behaviors we see around us, or to reject them consciously. We likewise learn to negotiate privacy choices as we see them reflected around us.

Two linked problems of (particularly digital) information environments: they fail to show us their extent or their duration.[86] Both persistence and accessibility can decontextualize information, allowing it to be taken out of the setting in which it was uttered and presented in unexpected ways.

When computers, or computer-assisted entities, aggregate data, they rarely provide meaningfully complete feedback.[87] They do not show us how they or their human principals perceive the aggregate data they've collected. aggregators amass and mine detailed long-term profiles from limited shared glimpses; online social networks leak information through continuous feeding of social pathways we might rarely activate offline; cell phones become fine-grained location-tracking devices of interest to governments and private companies, unnoticed until we map them.[88] These aggregators rarely give us comparative views by which we can re-norm our behavior or correct for unwanted information leakage.

[85] This despite being poor mental statisticians, see Tversky and Kahneman, *supra* note **??**

[86] See danah boyd, "Making Sense of Privacy and Publicity." SXSW. Austin, Texas, March 13 2010, "Unfortunately, online environments are not nearly as stabilized as offline ones. While the walls in the streets may have ears, digital walls almost always do. More problematically, online architectures have affordances that are quite different than offline ones - persistence, searchability, replicability, scalability."

[87] "When it comes to a lack of trust, the worst offenders of all are today's electronic devices [and, he could add, social Web], especially the computer (although the cell phone is rapidly gaining ground). The problem here is that you don't know what to expect. The manufacturers promise all sorts of wonderful results; but, in fact, the technology and its operations are invisible, mysteriously hidden from view, and often completely arbitrary, secretive, and sometimes even contradictory. Without any way of understanding how they operate or what actions they are doing, you can feel out of control and frequently disappointed. Trust eventually gives way to rage." Norman, *supra* note **??**, p. 140-141.

[88] Kai Biermann, *Betrayed by our own data*, March 2011.

Privacy depends on social feedback and flow-control. We can take responsibility for our privacy choices only when we understand them, and we can understand them best through seeing them operate. Facebook's newsfeed sparked outrage when it launched by surprise, but as users saw their actions reflected in feeds, they could learn to shape those streams to construct the self-image they wanted to show. Other aspects of interface design can similarly help us to manage our social privacy.

3.3 Feedback Control

Technologies and interactions that give us feedback about the publicity of our actions give us a degree of control. On the first level, the control may be limited to "accept or exit," but even that choice may be more granular: how much to share, how to hide or segment communications. The visible lack of privacy in a space where we'd like it can prompt a second-level response, a demand for change.

Social networking sites provide a wealth of examples of feedback success and failures. Facebook's newsfeed, an aspect of the site's peer-to-peer sharing, provides good feedback about what friends can see. Status updates a person posts to Facebook show up both on her profile and on a newsfeed for all of her friends,[89] where they are aggregated with each friend's other updates, application notifications, invites. The newsfeed spurred outrage when it was introduced–it seemed spooky to see a moment-by-moment chronicle of one's actions on the site, updated in real-time–but users quickly adapted (and some left). Seeing the appearance of friends' updates cued users how to manage their own statuses. [[Watch the spread of memes, e.g. users on twitter developing hashtags and @s, which the software then incorporated and built upon.[90]]] The newsfeed was not new information, it was an aggregation of existing material, and it was symmetrical – you could now see quickly and relatively thoroughly what Facebook and your friends could see. If you found it embarrass-

[89] In recent updates, Facebook has permitted users to select subsets of friends.

[90] Research on the linguistic convergence of a group, or patois?

ing to see a friend's breakup status broadcast, you could learn from that experience to mute your own relationship news, or use the feed toggle explicitly to signal availability.

In contrast, Facebook settled a complaint from the Federal Trade Commission over several information-sharing practices–sending information to applications or advertisers–that were less transparent. The Complaint alleges that Facebook shared information with apps and advertisers even if the user had designated it "Friends only" in the interface. This information flow was non-transparent and non-reciprocal. It diverged from and exceeded that which users would think they had permitted with explicit privacy settings.[91]

In settlement, Facebook agreed that "prior to any sharing of a user's nonpublic user information ... with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s) [it would] clearly and prominently disclose to the user" the categories of information, the identities of the share-ees, and "that such sharing exceeds the restrictions imposed by the privacy settings."[92] Facebook agreed to obtain express affirmative consent to these overrides.

In oversharing, Facebook was not only ignoring its users' stated preference, it was making that choice without notice or feedback to the users. Whereas all users had access to newsfeeds and profiles showing status updates, most were in no position to see what information was disclosed to application-developers. (A few applications, such as TKTK offered to show this for a user's own profile, but even those did not show that apps had access to any *friends'* information as well.)

That the newsfeed represents peer-to-peer privacy or disclosure, whereas applications and advertising disclosures are peer-to-corporation, hints at the divergent incentives that

[91] "None of the pages [of privacy settings] have disclosed that a users choice to restrict profile information to 'Only Friends' or 'Friends of Friends' would be ineffective as to certain third parties. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to 'Only Friends' or 'Friends of Friends' accessible to any Platform Applications that the users Friends have used." Federal Trade Commission, 'Complaint, In Re: Facebook, Inc.', *supra* note **??**, ¶14

[92] Idem, *Consent Decree, In Re: Facebook, Inc.* November 2011 ⟨URL: http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf⟩, p. 4-5.

can affect feedback-provision. Advertisers and apps, who pay Facebook's bills, want access to user-information but don't necessarily want to provide feedback along with it, especially if it would encourage users to adapt by sharing less.[93]

3.4 Designing Feedback

"An information-feedvack system esists whenever the environment leads to a decision that results in action which affects the environment and thereby influences future decisions."[94]

What does good feedback look like? We can find principles for feedback in human-computer interaction, design, and systems literature.

> An important component of understanding comes from feedback: a device has to give continual feedback so that a user knows that it is working, that any commands, button presses, or other requests have actually been received. This feedback can be as simple as the feel of the brake pedal when you depress it and the resultant slowing of the automobile... To be effective, feedback must enhance the conceptual model, indicating precisely what is happening, and what yet remains to be done. Negative emotions kick in when there is a lack of understanding, when people feel frustrated and out of control–first uneasiness, then irritation, and, if the lack of control and understanding persists, even anger.[95]

Good feedback is responsive, near to the event that causes it, both in time and space, so we recognize it; proportionate to its stimulus and consequences; salient; transparent;

- Responsiveness. Reflective symmetry? Visibility.
- Timeliness. If feedback is subject to delay between condition and response, it can cause systematic oscillations as participants overshoot and retreat. It may not even be visible as feedback. [Systems and cognitive properties]

[93] Consider Do-Not-Track. Advertisers may move toward self-regulation through disclosures if they fear impending regulation of a more disruptive nature. Even the feedback mechanisms they have have added, little triangles, i's and "ad preference" links, is hardly conspicuous.

[94] Forrester, *supra* note **??**, p. 14.

[95] Norman, *supra* note **??**, p. 76-77.

- Continuity. [Consistent or intermittent? cognitively, intermittent reinforcement, a la Pavlov's dog is more effective [in some circumstances] we don't become inured to it. (reward? which circumstances?) Yet for predictability and planning, consistency helps.
- Frequency. It has to be hit frequently enough to stick, be noticed.
- Relevance and proportionality. Feedback matches the impact of the action. (Google's notice-bar at the top of its properties, serves as warning of potential tracking)
- Consistency with outside experience[96] (intuitive to newcomers; balance consistency and ease-of-access with experience-rating, warning fatigue, to keep the right level of engagement)
- Coherence within the environment (a button always behaves the same way) (sometimes you'll want to change it to get attention. Cf Japanese researchers on "unfamiliar environment promotes health)
- Experience-rated? (Fits Norman's conceptual modeling of experience: we don't have to learn how to use each new object we encounter, but as we use something frequently, we can optimize it.) appeal to both the novice and the expert. (learn from online games, where you get new skills, encounter new items as you are prepared to use them [at least those games not designed around selling power-ups])
- resistant to warning fatigue (Perrow)
- self-constraining options (e.g. Google beer-googles; MS "do you really mean to send that?")
- Customizability? (stop warning me already) cf Ayres.

Many of the "nudges" suggested by Thaler and Sunstein's libertarian paternalism amount to better feedback.[97] Better is more immediate, describing options and outcomes in meaningful terms, with opportunities to review and repeat choices. Feedback supports many of the principles in the privacy-by-design framework propounded by Ann Cavoukian: it is preventative, default, embedded, transparent, and centered on the end-user.[98]

Of these, privacy feedback poses several challenges.

[96] D.A. Norman, *The design of everyday things*, (Basic books, 2002).

[97] Thaler and Sunstein, *supra* note **??**.

[98] Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles', (2011) ⟨URL: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf⟩.

Timing: Feedback about tech's privacy impact can be very far delayed, especially when new techniques or auxiliary information are added to old "disclosures." Old photos can be tagged with ID, old court records scanned and made much more easily searchable. Yet there are bright spots, Google's forward secrecy protects current conversations against future improvements in cryptanalysis. [99] Responding to these jumps is not just a matter of recognizing technological phase-change, but devising social and legal strategies to contain it. We will encounter such surprises more frequently as the pace of technological change accelerates.

Feedback problem when the technology changes too fast for our expectations to keep up. We shape our behaviors by what we see the technology do for our environment, but there's a transition period while we're adapting to changed tech. Some of our expectations are in fact set by the visible breaches of earlier expectations, and their consequences. (cf heuristics, some of the worse effects are more salient. do we ask the early adopters to 'take one for the crowd' by getting stuck? or do we think their behaviors won't be close enough to mainstream for that to be a learning example?)

3.4.1 Two-Sided Privacy: Dealing with incentive skew

Just as there are two-sided platforms, where different people interacting have different market goals, we can speak of two- or multi-sided privacy concerns, as users of a platform: we are concerned about privacy against peers, against the platform provider, and against the government. This is an architectural shift in degree that becomes one in kind: the proprietor of a store has access to information about us too, but the proprietor of a social network has both more information to aggregate and less-visible ways of gathering it.

The insights of two-sided networks help to explain why proprietors would give away products or access to services – because they're selling that audience to the other "side"

[99] See Adam Langley, "Protecting data for the long term with forward secrecy," http://googleonlinesecurity.blogspot.com/2011/11/protecting-data-for-long-term-with.html.

of the platform, whether it's credit card users or newspaper readers. Here, recognizing the different strategic positioning of the parties highlights information asymmetries that make information disclosures to different people mean [very different things]. Also, why platform providers may be particularly antithetical to particular kinds of activity – those which threaten their other-side markets. e.g. Apple refusing to allow apps that compete with it or the things its carriers value. What happens to a Facebook anti-behavioral ad group?[100]

Social networks as two-sided markets. Social networks carefully tune the feedback they offer us – but just not always toward *our* interests. These networks make their money only indirectly by pleasing us – and more directly (when they do make money) by selling us to advertisers.[101] Thus they look at metrics such as how many members they attract, how much time we spend on the site, and how frequently we return, but also how much demographic data we share, and whether we fit the categories advertisers value and follow their links to purchase (and thus encourage repeat advertising customers). Some market signals may be functioning, but unless we start getting better feedback about privacy, they are not helping us.

Finally, we might want to re-shape the space. not just offer information on the technological possibilities, but change the technology itself. we want semi-permeable membranes, giving access to friends and not to bosses or governors.

3.5 Systems of Privacy

TK Expand or delete

[100] See Rebecca MacKinnon, Consent of the Networked (2012).

[101] Here, we can look at the economic literature on two-sided markets or platforms. Economists recognize that as a platform proprietor plays between two sets of often divergent interests, it may make choices that limit the options of one client "side" or the other. Thus Facebook and other social network sites groom their users into an attractive audience for advertisers, emphasizing "family friendly" (and advertiser-friendly) content over violent or controversial material – even if that material is in the service of the Arab spring, how many advertisers want their "buy now" offers appearing next to a scene of self-immolation?

Feedback is also a property of systems. And Privacy, or the lack thereof, should similarly be seen as a system property, where a given individual's privacy is determined by aspects of the environment and the actions of others, as well as his own choices. Speaking in systems terms, the privacy along any edge/link is a function of the system's organization as well as of individual choices.

Feedback enables a system to self-correct. Enables the parts of a distributed system to coordinate without central direction and control.

A system has flows governed by regulators. In a balanced system, the regulators give feedback toward equilibrium. In an unbalanced system, feedback is missing or in the wrong direction, and the system spirals out of control. But that's too goal-directed- a system doesn't have goals. but we within it can, and can see when the system fails to match our goals.

A system with no regulation is liable to spiral out of control, until it hits a different constraint. Yet the regulatory answer need not be law. Law is but one method of regulation, see Lessig, Simon. Some mechanisms can operate closer to the potential problem.

If our goal is to preserve privacy, we should look for regulators that will help to do so. In particular, we search for mechanisms that give feedback to the system's actors about their behavior (reinforcing positive, damping negative). [102] Feedback, in the right direction, . Anything can serve as a regulator of flows , law, tech, markets, norms. in Lessig's taxonomy. Feedback can be simple or complex: the temperature sensor in a thermostat that triggers heat when the temperature drops too low, or cooling when it rises too high, is an equilibrating feedback. More complex ecosystem feedback , the predator-prey cycles: too many deer destroy the vegetation, weakening and falling prey to disease and wolves/coyotes, who get more numerous, until they thin the deer herd. Removing the wolves entirely may help the ranchers protect their cattle, but also swells the deer popula-

[102] Criminal law's punishments are a form of feedback; civil law's restitution or equity.

tion to unsustainable levels, and brings other unexpected changes.

4 Law and Feedback

Does the law currently provide privacy-feedback? In the U.S., where the law is famously sectoral and fragmented, we can find it in places: the Fair Credit Reporting Act requires customers to be able to get free annual credit reports[103] and provides that consumers who have credit scores used against them are entitled to see those scores – feedback at a time highly relevant to them, although too late to recapture that loan unless they can point out an error in their score. The Federal Trade Commission has put enhanced notice provisions into recent consent decrees. But no laws provide responsive feedback as an individual makes privacy-relevant choices.

Law does better (and could do better still) to enable others to provide feedback. Legal requirements of notice build a scaffolding on which third parties can report the features of that notice (e.g. EFF's TOSback); laws requiring data transparency or access can permit third parties or applications to monitor data collection and reflect its uses back to individuals.[104] [105]

Kyllo meet the net, again. We adapt behavior to the reasonable expectations of privacy that technology provides. Changes on different time-scales challenge these feedback mechanisms. Our use-driven feedback gets confused when the technology changes *as* our behavior does. Attribution error - causation or not?

Ratchet down: companies should only be permitted to make their tech more privacy-protective, not less. Compare Google+ to Facebook (or Buzz).

[103] Get them from annualcreditreport.com, not from other sites that fraudulently advertise them "free" with purchase; see http://www.ftc.gov/bcp/edu/microsites/freereports/index.shtml.

[104] J. Donath et al., 'Data Portraits', in: *ACM SIGGRAPH 2010 Art Gallery*, ACM (2010).

[105] The European Data Directive

4.1 Failures of Notice and Consent

The standard models for consumer and online privacy in US law focus on notice and consent and reasonable expectation of privacy.[106] The Fourth Amendment protects us from warrantless searches in areas where we have a "reasonable expectation of privacy."[107] Against private parties, both individual and corporate, as well as against non-investigative government data collection, the fair information practices paradigm has called for notice and consent.

For example, California's "privacy policy" Cal. Business and Professions Code 22575(a) requires that "(a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site," so that individuals can make informed decisions whether or not to continue using the site or service.

4.1.1 Notice Is Necessary but Insufficient for Feedback

Is a posted privacy policy feedback? Not in the way that I mean it (nor in the way that designers or systems analysts use it). [108] A privacy policy is static. Even if it forces a user to scroll through it to reach an "agree" button, past "conspicuous" provisions in all-caps type, it is not responsive to anything the user does (beyond failure to "agree" which may deny access to the site). Once clicked-through, it is generally forgotten, if it was even read the first time.

Good feedback is dynamic, responsive to the user's actions. It differs depending on

[106] Solove, Schwartz, Cohen, etc.

[107] This protection is limited further by exceptions such as the "third party doctrine," which deems us to have minimal or no expectation of privacy in information voluntarily disclosed to a third party, even as a condition of its effective conveyance; and by poor tracking between expectations and technological possibility.

[108] See Norman, Simon; see also R.S. Whitt, 'Adaptive Policymaking: evolving and applying emergent solutions for US communications policy', *Fed. Comm. LJ*, 61 (2008), p. 502n96 (describing "'feedback' as transparency (information) plus accountability (responsibility)."

what the user does to provoke it. Whereas notice–whether a bright warning sign or a barely-visible link–is static (generally so; dynamic warnings, triggered when an individual comes close to taking action, are a notice-like form of feedback).

Norman's design principles for usability distinguish "visibility" and "feedback."[109] Although the two are complementary, they serve different functions. Visibility offers static indicators for actions (push, pull, click) and describes their consequences. Feedback is dynamic, what gets reflected back in response as the user takes one of these actions. Together, a well-designed object or system cues the user toward potentially useful actions and then permits the user to verify that the machine is working as desired and to evaluate the effects of actions on it. A privacy notice may, if seen, give the user cues, but without feedback either whether the notice accurately describes privacy practices or on what happens when data is used according to those descriptions, it fails to be usable.

Feedback is more robust than mere notice.[110] Ryan Calo tries to "rehabilitate" notice by making it interactive, but at the cost of terminological clarity, mixing cause and effect. He speaks about user experience, but his "visceral notice" straddles the notice-feedback line, since it rarely varies with changing user input.

Used right, feedback can help create a self-regulating privacy ecosystem. (ha!)

4.2 Feedback Loops

Feedback that reminded us about all the tracking and profiling possible could over-inhibit us. We do not want to be conducting all of our social interactions on terms we'd be happy

[109] Norman, *supra* note **??**, p. 4-10.

[110] To the extent that Ryan Calo argues for "experience" as a form of notice, he is really blurring the category. "Indeed, experience itself can constitute a kind of non-linguistic or 'visceral' notice, altering expectations and understanding while avoiding many of notice's apparent pitfalls." M. Ryan Calo, 'Against Notice Skepticism In Privacy (And Elsewhere)', (2011) ⟨URL: http://www.futureofprivacy.org/wp-content/uploads/2011/07/Against%20Notice%20Skepticism.pdf⟩, p. 4, Victoria Groom and M. Ryan Calo, 'User Experience as a Form of Privacy Notice: An Experiment', (2011) Sometimes he uses "experience" to mean non-verbal forms of notice, while at other times he uses it to mean experiential *changes* in response to an individual's actions. Only the latter gives feedback.

to see on the front of the New York Times or Twitter's "featured tweets." But regulation of our private behavior to suppress communication isn't the only possible response to a full view of technology's intrusion: We could adapt new behaviors that protect us from out-of-context snoops but are transparent to our friends. We might use encryption more; or we might use law.

We could switch to technologies that offered more granular protection, or use the threat of switching to induce those we currently used to add better controls.[111] When Google Plus launched with "circles" offering greater context-controls for sets of friends, within weeks, Facebook responded with friends lists allowing similar sub-categorization. Whether this is this copying or parallelism doesn't particularly matter for our analysis.[112] Yet all this is regulating the peer-to-peer contexts (and their separability). One could say that it's partly because the feedback on those contexts is more immediate and salient. Diaspora*, the distributed social network that includes as explicit feature the lack of centralized knowledge or a proprietor with the ability to betray privacy, has had a difficult time reaching public use at sustainable scale.

4.3 Law to Change Tech to Change Privacy

Sometimes, better feedback on the privacy-invasive potential of technology will induce us to seek solutions outside of the technology – in legal regulation (which can be either tech-neutral or tech-specific). It can prompt meta-feedback. [113]

So the advent of the telephone, and courts' reluctance to grant it Fourth Amendment shield, prompted wiretap laws. Now, recognition of the pervasive use of computer and

[111] A.O. Hirschman, *Exit, voice, and loyalty: Responses to decline in firms, organizations, and states*, (Harvard Univ Pr, 1970).

[112] Although it prompts questions about network effects and the ability to change the cognitive background. Simon noted that social evolution is "Lamarckian" because organizations can copy from one another. Although, more recent plasmid biology shows opportunities for that chunked transfer in nature too.

[113] Compare the interaction of modalities of regulation in Lessig's Code: law can influence or be influenced by architecture, norms, and markets, a "regulatory two-step." Lawrence Lessig, *Code and other laws of cyberspace*, (Basic books, 1999), p. 90-99

electronic communications has led to concern that these laws, as modified in 1996, do not go far enough. Moreover, such concerns motivate the companies themselves. As they want to offer a better product to their users, one that protects them better from government intrusion, many have come out in support of ECPA reform. Sometimes the market forces work to produce law – although it's too early to say whether they will in this case.

Another form of legal regulation comes through the Federal Trade Commission's enforcement authority against "unfair and deceptive acts and practices." After identifying and preparing complaints against arguably deceptive privacy practices, the FTC has entered consent decrees with both Google (Buzz) and Facebook. The consent decrees can and do go beyond Section 5's reactive enforcement: each company has signed up for a 20-year period of enhanced reporting around privacy practices. As market leaders find themselves subject to higher scrutiny, these large network proprietors now face different incentives: to respect privacy and to force their competitors to do so as well – either through statutory or administrative agency law, or standards that become law.

While most of our examples have been from peer-to-peer and peer-to-company privacy, the lessons of feedback with the "reasonable expectation of privacy" that applies in the Fourth Amendment context against government search and seizure. In the GPS-tracking case of *U.S. v. Maynard*, currently before the Supreme Court as *U.S. v. Jones*, the DC Circuit held that "whether something is expose[d] to the public... depends not upon the theoretical possibility, but upon the actual likelihood, of discovery by a stranger."[114] Something "actually likely" to be observed by a stranger is not protected against warrantless observation by the police. Feedback through experience is what syncs "actual likelihood of discovery" with the absence of "reasonable expectation of privacy." If police could surveill everyone 24 hours a day but don't – it's possible but actually unlikely – few people have the experience of such surveillance to develop protective feedback, few cases get before

[114] *United States v. Maynard*, (615 F.3d 544, 2010), pp. slip op. at 25.

the courts to prompt legal limitation.

Consider *Kyllo v. United States*,[115], holding that use of a surveillance "device that is not in general public use" constitutes search for Fourth Amendment purposes. On the one hand, a) we don't want to exclude the police from what's generally available to the citizenry b) but if it's not generally in public use, the public hasn't had the opportunity to set limits on the device through means other than court intervention – eg. legislative.

The possibility of legislative override is a part of the judicial analysis and the democratic process of feedback. Hence California Gov. Jerry Brown missed the boat when vetoing state legislation (passed with an overwhelming majority) that would have required law enforcement to obtain warrants before searching cell phones.[116] After the state's highest court found warrantless search constitutional and the Supreme Court denied cert, the public expressed its dissent – and desire for greater protection of mobile phones– through legislation.[117]

The experience of both members of the public at-large and that of the Justices matters here. During *U.S. v. Jones* oral argument, Justices expressed concern that the Government interpretation would mean *their* cars were open to constant surveillance. Their later reflected that greater familiarity and the concern it bred.[118]

5 Feedback as Regulatory Support

Ours is a world of polycentric privacy, regulated by many different sources. Feedback supports adaptive, iterative policy-making[119] Notice and adapt has higher option value than

[115] *Kyllo v. United States*, (533 U.S. 27, 2001).

[116] See "Calif. Governor Veto Allows Warrantless Cellphone Searches," Wired, Oct. 10, 2011 http://www.wired.com/threatlevel/2011/10/warrantless-phone-searches/ "The courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizure protections," the governor wrote, puzzling many.

[117] SB 914, http://info.sen.ca.gov/pub/11-12/bill/sen/sb_0901-0950/sb_914_bill_20110902_enrolled.html

[118] **?**, .

[119] Whitt, *supra* note **??**.

notice and choice (of exit).

Feedback enables self-regulation, not at the level of corporate intermediaries, but at the level of the individual. Thus we might consider feedback-enabling transparency and legal regulation as substitutes: either one can function to give individuals privacy, but with different characteristics.

Transparency-enhancing feedback is more demanding than mere notice. As compared to government regulation of applications' data collection and use, a transparency mandate can allow for more flexibility at the application-development level. Developers can choose what to do and how to implement their disclosures of those practices. [of course their choice is not totally unconstrained] This leaves room for innovation in both the services and the manner of explaining them. Some innovations will not meet the legal level, but those can be rooted out post-hoc?

As technology and Internet companies argue against intrusive privacy "regulation," they have the tools to stave it off by providing real means and opportunity for their end-users to self-regulate. Where it works, feedback-aided self-regulation on the individual level can be better tuned, less costly, and more effective than a global privacy mandate.

5.1 When Feedback Fails

Self-help self-regulation may be a first choice, but we call upon law when that fails. Privacy-feedback failure can take two opposite forms: when it fails to alert us to objectionable information disclosures, or when it gives us good notice of objectionable properties.

Privacy control depends on meta information flows. To manage it, we need to know how our information will be used, how it will constrain our choices. Transparency enables feedback. A law or tech whose operation is transparent to those affected by it enables feedback on the regulatory mechanism itself and on the system around it.

So transparency of the law implies citizen understanding of the terms of the law and

conditions within which it operates. It also implies visibility of the law's operation and its effects on citizens. A law that is on the books but rarely enforced is less transparent than one regularly invoked. (and thus its sudden enforcement could be arbitrary and unfair) (compare the purpose of "open and notorious" possession in the law of adverse possession. There's an opportunity for self-help feedback along the way, that's not present if someone is silently waiting for a decade to pass.) (The problem of hidden terms in contracts of adhesion, that we don't get feedback at a relevant time in our decision-making.)

Non-transparency hides the linkages and steps between incident and catastrophe. Would better feedback enable us to decouple the system? to break chains and contain the failure?

5.1.1 Notice failure.

The many reasons for notice failure are well cataloged, including unreadable privacy policies (Macdonald, Cranor); bad experience engineering. (consider security analogies, Dhamija); Behavioral limitations and bounded rationality. Also, note that people do not tend to correct their heuristics because they don't code their experiences in such a way as to recognize and self-correct.

"Statistical principles are not learned from everyday experience because the relevant instances are not coded appropriately. ... A person could conceivably learn whether is judgments are externally calibrated by keeping a tally of the proportion of events that actually occur among those to which he assigns the same probability. However, it is not natural to group events by their judge probability."[120]

In other words, for people to self-correct judgments, biases, or behavior, we must get feedback in meaningful form. If the effects of information disclosures are concealed, we cannot make those adjustments.

[120]Tversky and Kahneman, *supra* note **??**, p. 598.

5.1.2 Choice failure.

The opposite problem can be equally troublesome: If the system gives proper notice of its lack of privacy, we may over-correct. (N% of people in Pew surveys who don't use Internet technology or social media because they're concerned by its lack of privacy; market research, some still don't use credit cards online.)

Personal and social value of privacy. amplification of the signal causes divergent responses, either withdrawal from the technology or dismissal of the threats ("get over it"), or security fatigue.

5.2 Pathologies of positive feedback

Finally, law itself is subject to systematic feedback effects. Law that is open to negative feedback, towards equilibrium, will be more self-correcting, hence better than that which does not. The First Amendment's protections of minority rights provide equilibrating feedback, by enabling the minority to speak out against changes that would disadvantage it.

Compare two kinds of informational control that have been classed under the right of privacy: defamation and publicity. I argue that the law of defamation incorporates negative, normalizing feedback, while law of publicity is subject to reinforcing positive feedback. (The names are potentially misleading; negative feedback is better at equilibrating than positive.[121]

Defamation law promotes control of reputational information by protecting people against false statements of fact harmful to their reputations. Any person is entitled to call upon the legal mechanisms of reputation-protection, but as the subjects' power and visibility grows, their legal protections weaken, and the corresponding First Amendment

[121] John Howard Miller and Scott E. Page, *Complex Adaptive Systems: An Introduction to Computational Models of Social Life*, (Princeton University Press, March 2007), ISBN 9780691127026, p. 50 "In a system with negative feedback, changes get quickly absorbed and the syste4m gains stability. With positive feedback, changes get amplified leading to instability."

protections for their critics increase. Someone who can call upon other channels to defend himself has less need of the law, [and, under a non-optimal system, more chances to control it.]

The public figure gets less protection from the law of defamation. He can still invoke its protections against malicious intentional falsehood, but not against mere negligence or carelessness. Instead, his critics are empowered in their complaints, even if they sometimes cross the line from truth to falsehood by mistake. Newspapers are told that they need not spend every last dollar to protect the powerful.

This is a negative, damping feedback loop: As one's power grows in public importance, either generally or to a particular subject to discussion, his power to invoke the law's protection shrinks. The person is faced with the choice: to rely on public fame or private law. [involuntary public figure?] Because the public figure has other channels for self-defense, the field is kept relatively balanced. The law helps to keep the marketplace of ideas open to all comers, those with more power to grab attention and those with less. The barriers to entry are lower than they would be if the rich could set the terms of debate as well as grab its attention. quote NYT v. Sullivan.

The law itself is partially kept in check by this dynamic – the info-rich are kept from becoming too powerful, and from gaining greater ability to influence the law through the use of defamation suits against their critics. Some states go further by enacting anti-SLAPP (Strategic Lawsuits Against Public Participation) laws.

Contrast the growing law of publicity, which provides a positive-feedback loop, a vicious spiral of "rich get richer." For it protects only the haves – you get protection only if you already have fame – commercial value of your image. [[And dilution law in general]] Publicity protects the pocketbook, [Prosser] the right to control commercial use of your image means most when your image already has commercial value. The user of a nobody's face is not trying to exploit his fame, while the user of a star's image is presumed to be

doing so. Three Stooges on a T-shirt. (but occasionally, Lamparello v. Falwell) This rich-get-richer dynamic (increasing returns to scale) in turn gives celebrities the means to put pressure on the law to help them get richer still. California only recently changed its law to extend the protection of publicity rights post-death – no incentive to the dead celebrities, but a monetary boon to the estates supporting campaigns in the state.

6 Conclusion

To be written!

Feedback: pluses and minuses

- + Adjustment, re-norming
- + transparency of regulation to end-users
- - undue caution
- - asymmetries of information, power, know-how amg users of sys
- - interdependence
- - problematic wrt absolute values, rights

References

Dwyer v. American Express, (652 N.E.2d 1351 (Ill. App. 1995), 1995).

Kyllo v. United States, (533 U.S. 27, 2001).

"Here Is a Human Being: At the Dawn of Personal Genomics", (HarperCollins, 2010).

'A Weinergate timeline', *Salon*, (2011) ⟨URL: http://www.salon.com/2011/06/01/weinergate_timeline/⟩.

United States v. Jones, (http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf, 2012).

Olmstead v. United States, (277 U.S. 438, 1928).

Katz v. United States, (389 U.S. 347, 1967).

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

Acquisti, Alessandro and Grossklags, Jens, 'Privacy and rationality in individual decision making', *Security & Privacy, IEEE*, 3 (2005):1, pp. 26–33.

Angwin, Julia, 'The Webs New Gold Mine: Your Secrets', *Wall Street Journal*, (2010) ⟨URL: http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html⟩.

Arrow, Kenneth, *Economic welfare and the allocation of resources for invention*, 1962.

Baldwin, C.Y. and Clark, K.B., *Design rules: The power of modularity*, Volume 1, (The MIT Press, 2000).

Biermann, Kai, *Betrayed by our own data*, March 2011.

boyd and Marwick, Alice, '"Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies"', (2011).

Brin, David, *The Transparent Society: Will Technology Force Us To Choose Between Privacy And Freedom?* (Basic Books, June 1998), ISBN 0738201448.

Calo, M. Ryan, 'Against Notice Skepticism In Privacy (And Elsewhere)', (2011) ⟨URL: http://www.futureofprivacy.org/wp-content/uploads/2011/07/Against%20Notice%20Skepticism.pdf⟩.

Cavoukian, Ann, 'Privacy by Design: The 7 Foundational Principles', (2011) ⟨URL: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf⟩.

Cohen, Julie E., 'Examined lives: Informational privacy and the subject as object', *Stan. L. Rev.* 52 (1999), p. 1373.

Crumlish, Christian and Malone, Erin, *Designing Social Interfaces: Principles, Patterns, and Practice s for Improving the User Experience*, (O'Reilly Media, Inc., September 2009), ISBN 9780596154929.

Dixit, A.K. and Pindyck, R.S., *Investment under uncertainty*, (Princeton University Press, 1994).

Donath, J., 'Signals in social supernets', *Journal of Computer-Mediated Communication*, 13 (2007):1, pp. 231–251.

Donath, J. et al., 'Data Portraits', in: *ACM SIGGRAPH 2010 Art Gallery*, ACM (2010), pp. 375–383.

Duhigg, Charles, *The Power of Habit: Why We Do What We Do in Life and Business*, (Random House, February 2012), ISBN 1400069289.

Dwork, Cynthia, 'Differential privacy', *Automata, languages and programming*, (2006), pp. 1–12.

Eckersley, Peter, 'How unique is your web browser?' in: *Privacy Enhancing Technologies*, Springer (2010), pp. 1–18.

Federal Trade Commission, *Complaint, In Re: Facebook, Inc.* November 2011 ⟨URL: http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf⟩.

Federal Trade Commission, *Consent Decree, In Re: Facebook, Inc.* November 2011 ⟨URL: http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf⟩.

Forrester, J.W., *Industrial dynamics*, (MIT Press Cambridge, MA, 1961).

Fried, Charles, 'Privacy', *Yale Law Journal* (1968).

Gannes, Liz, *The Apologies of Zuckerberg: A Retrospective*, (AllThingsD, November 2011) ⟨URL: https://allthingsd.com/20111129/the-apologies-of-zuckerberg-a-retrospective/⟩.

Gleick, James, *The information: A history, a theory, a flood*, (Pantheon, 2011).

Goffman, E., *Behavior in public places: Notes on the social organization of gatherings*, (Free Press, 1966).

Groom, Victoria and Calo, M. Ryan, 'User Experience as a Form of Privacy Notice: An Experiment', (2011).

Harford, Tim, 'One maths formula and the financial crash', *BBC*, April (2012) ⟨URL: http://www.bbc.co.uk/news/magazine-17866646⟩.

Hayek, F.A., 'The use of knowledge in society', *The American Economic Review*, 35 (1945):4, pp. 519–530.

Hippel, Eric von, '"Sticky Information" and the Locus of Problem Solving: Implications for Innovation.' *Management Science* (1994).

Hirschman, A.O., *Exit, voice, and loyalty: Responses to decline in firms, organizations, and states*, (Harvard Univ Pr, 1970).

Hull, J., *Options, futures and other derivatives*, (Pearson Prentice Hall, 2009).

Jolls, C., Sunstein, C.R. and Thaler, R., 'A behavioral approach to law and economics', *Stanford Law Review*, (1998), pp. 1471–1550.

Kahneman, Daniel, *Thinking, Fast and Slow*, (Farrar, Straus and Giroux, 2011).

Kerr, Orin S., 'The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution', *Mich. L. Rev.* 102 (2003), p. 801.

Knight, F.H., *Risk, Uncertainty and Profit*, (University of Chicago Press, 1921).

Laurie, Ben, 'Why Privacy Will Always Lose', *Links* (2009).

Lessig, L., 'The Architecture of Privacy', *Vand. J. Ent. L. & Prac.* 1 (1999), p. 56.

Lessig, Lawrence, *Code and other laws of cyberspace*, (Basic books, 1999).

McDonald, A.M. and Cranor, L.F., 'The cost of reading privacy policies', *ACM Transactions on Computer-Human Interaction*, 4 (2008):3, pp. 1–22.

Miller, John Howard and Page, Scott E., *Complex Adaptive Systems: An Introduction to Computational Models of Social Life*, (Princeton University Press, March 2007), ISBN 9780691127026.

Narayanan, A. and Shmatikov, V., 'Robust de-anonymization of large sparse datasets', in: *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, IEEE (2008), pp. 111–125.

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, (Stanford Law Books, 2009).

Norman, D.A., *The design of everyday things*, (Basic books, 2002).

Norman, Donald A., *Emotional Design*, (Basic Books, 2004).

Ohm, Paul, 'Broken promises of privacy: Responding to the surprising failure of anonymization', *57 UCLA L.Rev. 1701* (2010).

Peppet, Scott R., 'Unraveling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future', *Northwestern U. L.Rev.* (2011).

Perrow, Charles, *Normal accidents: Living with high-risk technologies*, (Princeton University Press, 1984).

Rosen, Jeffrey, *The unwanted gaze: The destruction of privacy in America*, (Vintage, 2001).

Schulmerich, M., *Real options valuation: the importance of interest rate modelling in theory and practice*, (Springer Verlag, 2010).

Schwartz, Barry, *The Paradox of Choice: Why More Is Less*, 1st edition. (Ecco, December 2003), ISBN 0060005688.

Shannon, C.E. and Weaver, W., *The mathematical theory of communication*, (University of Illinois Press Urbana, 1962).

Simon, H.A., *The sciences of the artificial*, (the MIT Press, 1996).

Solove, Daniel J., 'A Taxonomy of Privacy', *154 U. Pa. L. Rev. 477* (2006).

Sweeney, L., 'Uniqueness of simple demographics in the US population', *LIDAP-WP4. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA* (2000).

Taleb, N.N., *The black swan: The impact of the highly improbable*, (Random House Inc, 2007).

Thaler, R.H. and Sunstein, C.R., *Nudge: Improving decisions about health, wealth, and happiness*, (Yale Univ Pr, 2008).

Tversky, A. and Kahneman, D., 'Judgment under uncertainty: Heuristics and biases', *Science*, 185 (1974):4157, p. 1124.

Warren, S.D. and Brandeis, L.D., 'The right to privacy', *Harvard law review*, 4 (1890):5, pp. 193–220.

Whitt, R.S., 'Adaptive Policymaking: evolving and applying emergent solutions for US communications policy', *Fed. Comm. LJ*, 61 (2008), pp. 483–765.

Zittrain, Jonathan L., *The Future of the Internet–And How to Stop It*, (Yale Univ Pr, 2009).