

Critiques of Proposed FTC and Safe Harbor Regulations:

The FTC has proposed regulation concerning five principles: Notice, Consent, Access, Security, and Enforcement. The Safe Harbor Principles, following the EU Privacy Directive, add two more: Onward Transfer and Data Integrity. I review each in turn:

(1) Notice

Both the FTC recommendation and the Safe Harbor principles call for notice to consumers regarding the use of their information. According to the FTC: “Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.”ⁱ

According to the Safe Harbor notice principle:

“An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party... [FN: It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.]”ⁱⁱ

All participants in the debate over privacy believe that notice is important. Some believe this because notice is a prerequisite for other Fair Information Practices, others because full information is a necessary precondition for markets to operate efficiently.

But, despite the agreement, notice is hard. Notices can be divided into three types: those that tell people what they already know, those that tell people what they don't know but don't care about (and that thus don't change their behavior), and those that tell people what they don't know and do care about. Because different people know different things, there's necessarily some overkill, but only notices that fall into they third category are typically worth the effort.

The most likely scenario is the first one – that in our zeal to address all the potential uses and potential risks of information flows, we'll insist on overbroad disclosures. Regulators, and risk-averse businesspeople and lawyers, are notorious for adding warning upon warning, to the point that most contemporary contracts are masses of unintelligible small print that no one bothers to read. There's a risk that “everything is more important than everything else.” All too often, various regulators with different

interests at different times deem various things (disclaimers, limitations of liability, privacy, etc.) of great importance and require that each one be especially “clear and conspicuous.” This generally translates as being written in bold capital letters, resulting in a document with a profusion of emphasis that effectively emphasizes nothing, or a profusion of separate forms (like the blizzard of paper you sign when you get a mortgage) that are unreadable in their volume. Who’s to say that disclosure of privacy policies is more valuable to consumers than the disclosure of finance terms, limitations of liability, or the next flavor of the month.

An example of what can go wrong with overbroad notice is the Federal Aviation Administration rule that flight attendants review with passengers the operation of seat belts before every flight. When PSA attendants started their seat-belt spiel: “For those of you who have not been in a passenger car since 1962...” they were pointing out the absurdity of telling people what they already knew. They captured a dramatically increased share of passengers’ attention for the part of the talk that gave out useful information (like where the exits were). But within a few weeks, they had incurred the wrath of the Federal Aviation Administration and had to stop. It’s a sobering illustration of regulatory inflexibility that, forty years later, we’re still giving notice of how a seatbelt operates. Applying that paradigm across a fast developing information economy is daunting.

Litigation-averse business people may make this situation worse. Unfortunately, the likely corporate response to any notice requirement (and concomitant expansion of liability) will be to describe every possible problem that could arise as a result of information exchange. The result is likely to be about as readable (and about as helpful) as the typical corporate SEC filing – which is to say, not at all. Liability driven notices are commonplace – from the backs of baseball tickets to the pages of fine print included in the instructions of any consumer appliance. But warnings that you may get hit by a baseball at the ballpark or that you should be careful with power tools don’t make the world a better or safer place. Nor do they change real world behavior. (Has anyone ever looked at the back of a baseball ticket and said “No, you’re right. I might get hit by a ball and not be able to sue the baseball team, and so I’m not going to the game today?” Never happens.) Worse, by making the boilerplate so expansive, we make it much less likely that most people will read the material to learn about unexpected risks.

Regulatory burdens typically take the form of the Death of a Thousand Cuts. In this context, unfortunately, more is worse. The proliferation of notices and warnings numb us to the truly important warnings of serious and unexpected risks. But legislators, regulators, and advocates too often declare victory and go home, understandably failing to undertake the Sisyphian and unrewarding task of periodically reviewing regulations to ensure that they are still necessary and meaningful. (There’s a reason that legal codes inevitably get longer year after year.) Regulators need to balance their interest in a particular topic in view of the overall consumer experience, and be disciplined in determining which one or two items are really priorities for consumer consideration. Otherwise, privacy notices will become the digital mattress tags for the 21st century, unread and unloved.

A second concern is that educating people about a complicated topic that they don’t want to know much about like leading a horse to water. The “privacy policy” pages of most websites, along with their legal terms, are typically among the least trafficked. The statements distributed by merchants in monthly bills are widely disregarded by

consumers as more junk mail. The Platform for Privacy Preferences (“P3P”), intended to give consumers a fine-grained way of expressing their detailed privacy preferences on the web, has largely died on the vine, a victim of an overwhelming lack of consumer interest.

Aware of this situation, both privacy advocates and those skeptical of privacy regulations have expressed frustration over the lack of clarity of many privacy policies.ⁱⁱⁱ It’s hard to track all the information that we exchange, all the places it’s stored, and all the ways it’s used. The FTC has alluded to the difficulty: “[I]n light of the complexity of actual business practices and the myriad ways in which companies can handle personal information, it is difficult to categorize the many disparate information practices embodied in the privacy disclosures that were analyzed. Many Web sites have multiple information practices that differ according to the nature or source of the information at issue or the context in which it was collected.”^{iv} For example, companies frequently may have multiple policies that apply in different circumstances (perhaps one approach for a sweepstakes entry, another for making a purchase).

Like “plain-English” securities documents, “simplified” privacy policies are likely to still be heavy sledding. Before passing notice regulations, legislators should be required to attest that they have been able to read through the detailed disclosures regarding the storage and use of personal information mandated by Section 631 of the Cable Communications Policy Act of 1984. Even where written in a user-friendly fashion (crammed full of friendly pronouns, short sentences, and bold graphics), these disclosures include an irreducible minimum of complexity that few consumers will be interested in reading through.

This problem points up the tension between completeness and accuracy on the one hand, and brevity and readability on the other. The May, 2000 FTC Report acknowledged: “As with many consumer disclosures, there is a tension between providing full and accurate information about a site’s information practices and providing short and easily understandable disclosures that consumers are likely to read and understand.”^v In the online context, the information “transferred” and “collected” with virtually every visit to a site would include a user’s operating system and its version number, their IP address (requiring a discussion of the difference between static and dynamic IP addresses, and how they differ from email address), browser type and version number, time-stamp information, prior web pages visited, information previously stored on the user’s last visit to a site, plus any information affirmatively provided by the user. Similarly, offline merchants may track purchasing patterns, buying codes, catalog versions and store locations, and the phone company or cable service may track (if only temporarily), significant amounts of technical information incident to your receipt of service. It may be a worthy effort, but no one should hold out too much hope for sterling results. Ultimately, regulators will need to do extensive line-drawing as to what information transfer must be disclosed.

Trying to cut this Gordian knot, Commissioner Leary has called for disclosures of “greater clarity and comparability”.^{vi} He notes that “[s]ome standardization of the disclosures would allow consumers to compare more easily the privacy practices of different vendors”^{vii} This seems a reasonable approach, but it’s again easy to underestimate the difficulties entailed. The FTC analysis gives a laundry list of notice topics (what is collected, how it’s collected, how it’s used, what other entities do with it, etc.), and suggests a simple two-by-two matrix of uses, divided between “internal” and

“external” uses and “primary” (for the intended transaction) and “secondary” (marketing) uses. But is a transfer to a third-party agent “internal” or “external”? Is a notice of an recall “primary” or “secondary”? What about notice of a software bug? A software upgrade (which may include a bug fix)? Does it depend on whether the company stands to profit from the notice?

Standardized boilerplate (some of which has already been generated by industry efforts) is relatively unhelpful given the variety of business practices and types of information involved. By comparison, the labelling of food products – in a setting where there was general consensus on the need and the value to consumers, generally high consumer interest, and a relatively manageable number of criteria to be displayed – took years of negotiation and debate.

Even a requirement as simple as “reasonably prominent notice of the types of information gathered and the uses to which it is put,” if taken literally, could result in pages of information about the detailed technical information incidental to online transactions, while the discussion of uses risks being either so high-level as to be meaningless or so specific as to be mind-numbing. What is “reasonable” in this context? What degree of detail does a consumer need to know what’s happening? Without the sort of clear prioritization and line-drawing described above, years of rule-making and court decisions will be needed to sort this out. And even making the sweeping assumption that the rules are clear, the ever-changing nature of information exchange in response to new business models and new consumer demands will inevitably create new traps for the unwary and require a new corporate bureaucracy devoted to tracking information flows.

To minimize irrelevant legalese, and maximize the real-world effect of notices, any requirements should stress practices and risks that aren’t commonly appreciated. This is an admittedly floating benchmark that will shift over time as people learn more about new technologies and as technologies and business models continue to evolve. But common sense, the existing laws of negligence, and standard industry practice provide some guidance. Unfortunately, in the interests of avoiding a “privacy” problem, most current privacy policies typically tell consumer what they already assume: “When you put your information in the “shipping address” form, we will use it to ship the product you have ordered. We may share it with the delivery carrier for that purpose.” Some regulatory safe harbor that recognizes that all information need not be disclosed all the time would make such notices far more effective.

Such safe harbors may, of course, become default industry standards. (As Commissioner Leary notes, the FTC’s “Green Guides” on environmental disclosure have changed manufacturing practices, and arguably done so in a way that makes optimal use of market mechanisms.^{viii}) This heightens the importance of getting notice requirements right. Setting the rules for precisely what companies must disclose, and how they must disclose it, may have the effect of dramatically skewing business arrangements. Done wrong, such rules may undermine the benefits of information exchange described in Section II and incur many of the regulatory costs described in Section III.

(2) Consent / Choice

It has become fashionable for regulators to re-label what was once generally known as “consent” (suggesting a more positive agreement consistent with opt-out approaches) as “choice” (suggestion a more affirmative election consistent with opt-in approaches). The FTC Privacy Online Report argues that “[w]eb sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).”^{ix}

Regarding “choice”, the US-EU Safe Harbor Principles provide that:

“An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. [FN: It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.]”^x

“For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.”^{xi}

Both the FTC recommendations and the Safe Harbor principles seem to contemplate simple and discrete transactions, rather than the increasingly common longer-term and more multi-faceted relationships between companies and customers. And both leave the scope of “consent” somewhat unclear. If “consent” means that a user is agreeing to the purposes set forth in privacy notices, the “consent” requirement adds nothing. If means more than that, what? That a customer must affirmatively consent to any use even where notice given? Or consent to uses that are not expected (notwithstanding their disclosure in a notice)? But if so, what is the purpose and value of notice?

Commissioners Leary and Swindle have both highlighted the risks of an overly broad understanding of consent: a free-rider problem that is part of the larger inequities discussed in Section II.B. As Commissioner Leary put it in the context of online profiling:

“If mandated “Choice” simply refers to some mechanism whereby a consumer can either grant or refuse permission for online profiling, I would have no problem with it. A consumer should have the ability to exit the site before the fact of the visit becomes part of a profile. If, however, “Choice” means that a consumer can exercise this choice (either by opting out or failing to opt in) and still obtain the same benefits as a consumer less solicitous of privacy, it could be unfair. Consumers who object should not have a legally guaranteed right to “free ride”

on possible value and corresponding benefits made possible by the cooperation of those who do not object. Put another way, it should not be illegal to reward consumers who are willing to be profiled. The question of appropriate rewards or penalties attendant upon the exercise of various options can be extremely complicated.”^{xii}

In the more general context of online privacy, he noted:

“The Report recognizes, for example, that it may be appropriate to provide affirmative benefits if a consumer agrees to certain personal disclosures (Report at 61). If the collection of data is one thing that makes it possible for a vendor to offer lower prices, consumers who are particularly tender of privacy would otherwise be able to free ride on the value created by those who are not. (If a supermarket issues a card that offers discounts to people who use it, in exchange for compilation of useful data, consumer ‘choice’ surely does not involve the right to get the discount without supplying the data.) On the other hand, if the premium for permission to use information is too generous, or the penalty for refusal too severe, consumer ‘choice’ really involves nothing more than the ‘choice’ to refuse dealings with the vendor. The issue of what is or is not a reasonable price differential is complicated, but may be too difficult to bother with in a situation where a particular vendor competes with a number of others that have their own policies. Does this mean that reasonableness should depend on the market power of the vendor?”^{xiii}

Commissioner Swindle echoed the free-riding concern:

“What are the likely effects on online commerce of Mandated Choice? Would sites have to extend the same level of services and benefits to all consumers, regardless of whether some are unwilling to provide information? To the extent sites rely on the sale or use of information to offset the costs of providing services, would they discontinue services to all or to some consumers? Would all consumers have to pay more for services previously offset by the sale or use of information? Could sites shift costs only to those consumers who demand a higher level of privacy, whether in the form of fees for using the site or by reducing the level of benefits and services offered to those who choose a higher level of privacy? Or is privacy an absolute right so that all participants in online commerce—retailers and consumers—should bear the costs of Mandated Choice exercised by some consumers? If so, in the name of “Choice,” this legislation may reduce the choices available to consumers in the online market.”^{xiv}

Such free-riding choice, by letting consumers use a service but not provide information in “payment”, threatens businesses like the hugely popular Free PC, which can no longer provide a free computer and get nothing (or be forced to sell only low-value, untargeted ads) in return. It seems unlikely that eliminating such innovative business models (which, in the case of Free PC offer to help bridge the Digital Divide by providing free computers) would be in the public interest.

Perhaps the most controversial aspect of “choice” is the question of requiring customers to “opt-in” to the collection and use of their data rather than “opting-out” of such collection and use if they objected to it. Privacy advocates argue that opt-out

approaches put too much of a burden on consumers to protect their privacy. But opt-in approaches obviously burdens everyone who wants the advantages of sharing information.

Peoples' tendency to stay with the default option makes the question of "opt-in" versus "opt-out" privacy regimes critical. If a website chooses an "opt-in" regime, in which the permission box is pre-checked and users need to uncheck it to withhold permission, a large majority of users will leave it checked. If the site chooses an "opt-out" regime, in which the permission box is unchecked and users need to check it to give permission, a large majority of users will leave it unchecked.

In the real world, this behavior means that where we require "opt-in" models, most companies won't bother to solicit information. If only 10% of your customers are providing information, it's likely neither representative nor substantial enough for you to build a program around. So where we put the bar of "informed choice" in fact makes the decision for most Americans, and dictates whether or not others will even have the opportunity to provide personal information in exchange for perceived benefits. How we interpret the European requirement of "unambiguous" consent is critical to this equation.

The FTC and Safe Harbor positions in this area give cause for concern. The Safe Harbor requires "opt-in" consent for use of sensitive information ("medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual").^{xv} Its definition of "sensitive" information doesn't necessarily dovetail with American sensibilities. And its examples are pretty clearly only the camel's nose under the tent. And one can easily imagine a number of other categories of information that are arguably "sensitive": what books you buy, magazines you read, the clickstream traffic of your internet browser, what liquor purchases you make. In fact, the FTC has already said that "[o]pt-in procedures may be more appropriate where the information at issue is particularly sensitive – for example, the collection and use of children's personal information or sensitive medical information.... As noted below, hybrids may also have a role, combining elements of both opt-in and opt-out...."^{xvi}

The Commission went on to note with apparent approval a proposal regarding "hybrid" choice, which stated that "[w]here past expectations about the nature and use of information would be changed (e.g., in cases of a material changes [sic] in privacy policy or a merger of previously non-identifiable clickstream [data] with personally identifiable information), opt-in choice has been required. By contrast, where only future expectation [sic] are implicated (e.g., the prospective merger of PII and non-PII), opt-out choice has been provided."^{xvii}

But such heightened requirements are very much open to debate. "There is no consensus as to what constitutes 'sensitive' information, and the definition appears to depend on personal preferences.... There should be no special requirement of explicit consent for the use of such an ill-defined category of data.... The same features that may make information sensitive may also heighten the importance of its availability."^{xviii}

In some ways, the desire for "choice" and "consent" is a proxy for a desire to exercise more control over an increasingly complex world. But having to control everything is a hassle, and carries costs. Do you want to pay for programming that can no longer be presented for free? When you're online, do you want to be asked every five seconds

about a bit of data? People may say they want education and easy-to-use technological tools to take charge of their online privacy, but their actual conduct suggests that they're not willing to sacrifice anything for them.

Finally, the ambiguity of determining which uses are "beyond the scope of" or "incompatible with" the purpose for which data was collected again presents a problem. The question is very complicated and depends on a number of variables, with open-ended regulations inviting litigation and detailed regulations likely to get it wrong.

(3) Access

Regarding access, the FTC's online legislative recommendation is that "Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information."^{xix}

The US-EU Safe Harbor Privacy principles provide that: "Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated."^{xx}

The FTC's Report conspicuously refused to take a position regarding the range of thoughtful and detailed alternatives set out by its own Advisory Committee on Access & Security. The Committee had spelled out access alternatives of: (1) Total Access; (2) Default to Consumer Access; (3) a Case-by-Case Approach Including Sectoral Considerations; (4) Access for Correction.^{xxi} The Commission's response was Delphic: "The Commission believes that all of these implementation options will be useful to Web sites in developing procedures to facilitate consumer access to personal information collected from and about them, and that the options will be relevant to any determination as to the scope of 'reasonable access'."^{xxii}

But other language in the Report gives grounds for concern. In the words of Commissioner Leary: "the Report endorsed by the majority states flatly that 'the Commission believes that fair information practices require that consumers be afforded *both* an opportunity to review information *and* an opportunity to contest the data's accuracy or completeness – *i.e.*, to correct or delete the data.' (Report at 32). This is an extraordinarily broad claim, which could in many cases lead to vast expense for trivial benefit and which provides an ominous portent for the content of any substantive rules."^{xxiii}

The risk, of course, is the one identified in Section IIB – that of engineering a system of significant cost (ultimately borne by all consumers) to address the desires of a small fraction of the American public who are interested in looking at their credit reports.^{xxiv} Privacy advocates argue that such a system would make the data practices better by enforcing accountability. But part of the question is accountability against what? If the information isn't gathered in the regular course of business, it's unlikely to be used. And if it remains unused, the chances of misuse that harms consumers already would seem to be quite low.

Certainly, different degrees of access are appropriate for different types of information. Certain information is the basis for important decisions like the granting of credit; other information is trivial, and may not be used at all. An employee of a corner store may have noticed you on your last visit – should that be subject to inquiry? (“Did any of your employees recognize me on my last visit here?”) What about the phone records of local calls that your phone company keeps for a day? Surfing records that a website recorded 10 minutes ago, and won’t be keeping beyond your browsing session? Some information is easily gathered in real time through existing systems, other information is compiled only rarely or not at all. The Advisory Committee Report acknowledges these complexities as well as others, such as frequency of access, charges for access, and access to downstream participants who may have once received information.

There seems a social consensus that people should have the ability to review and correct important personal information about them on a regular basis – a consensus reflected in the Fair Credit Reporting Act of 1970.^{xxv} Beyond that, consensus breaks down rapidly. Certainly there’s the reflexive view that “I want to access everything about me.” But this fails to take into the costs of such a claim. All access all the time to everything is simply overkill. The Frequently Asked Questions section accompanying the Safe Harbor principles recognize these limitations: “[T]he right of access ... allows individuals to verify the accuracy of information held about them.... [T]he obligation of an organization to provide access to the personal information it holds about an individual is subject to the principle of proportionality or reasonableness.... Expense and burden are important factors and should be taken into account” although are “not controlling”.^{xxvi} The Safe Harbor principles therefore require access only when it “is readily available and inexpensive to provide” unless the information is sensitive or used for decisions that “significantly affect the individual”^{xxvii} Moreover, “[a]ccess needs to be provided only to the extent that an organization stores the information.”^{xxviii}

Finally, the access issue provides a concrete example of the difference – and tension—between privacy and security. In a statement concurring with the Advisory Committee report, Stewart Baker noted “[a]s the Report says: ‘Giving access to the wrong person could turn a privacy policy into an anti-privacy policy.’ If access to personal data is turned into a legislative right, Americans’ personal data will be at risk of exposure to con men, private investigators, suspicious spouses – anyone who has the *chutzpah* and the scraps of information needed to plausibly impersonate their target.” Mandating access under these circumstances creates a risk of liability for companies damned if they require clear and convincing proof of identity before giving access, and damned if they don’t and are exploited by a con man. While there is thus a need for liability protections, and a safe harbor for access practices, the reality of American litigation means that the combination of access standards and safe harbors will effectively become requirements, driving business practices in ways that may not clearly benefit consumers.

(4) Security

The FTC final online legislative recommendation is that: “Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.”^{xxix}

Similarly, the Safe Harbor principles provide that: “Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.”^{xxx}

Security (especially “reasonable” security) is obviously a fine idea. And it was the only point of consensus among the variety of experts represented on the FTC’s Advisory Committee. But neither is there compelling evidence that the government needs to take a role: “The Committee did not hear any evidence that consumers had actually suffered significant losses from exposure of their personal data on the Internet (it appears that losses from the well-publicized hacker thefts of credit card information fell mainly or exclusively on merchants and banks.”^{xxxi} Any security requirements specified by security are likely to be expensive and not well tailored to the needs of any individual company. They will therefore likely exclude at least some smaller competitors from the marketplace.

Consumers can already sue a company whose system was hacked, alleging that it was negligent or spent too little money to ensure the security of its systems. Such private sector enforcement – again, coupled with adverse publicity, which may take an even steeper toll – is the real enforcement mechanism for meaningful security. It is difficult to imagine a form of security notice that would be detailed enough to give reasonable comfort while still being intelligible to most users and not disclosing information useful to those interested in breaking in. In the related context of security for federal computer systems, such disclosure has been harshly criticized: “Why would an arm of the government spread the word about vulnerabilities that ‘put critical operations and assets at risk’ in a report that is available for the reading pleasure of very cracker, hacker, and terrorist from here to Libya?”^{xxxii}

Over time, if security becomes a concern for consumers, privacy sector security audits will likely become more common, producing a kind of Good Housekeeping Seal of Approval for security practices. But since security is typically more a matter of individual behavior rather than the technology and systems in place, third parties may be uncomfortable certifying another’s security practices, making the risk harder to insure against and driving up costs. But we’re a long way from that particular market failure, and it’s not at all clear that the FCC rather than a professional information technology group is in the best position to set benchmark security standards.

(5) Enforcement

The FTC has not laid out its position on enforcement, but presumably envisions receiving civil and criminal enforcement authority. Moreover, statutory benchmarks or regulatory benchmarks or safe harbors could, expressly or implicitly, create private rights of action for any variance from their terms.

Regarding enforcement, the Safe Harbor Principles provide that:

In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations

to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.^{xxxiii}

Enforcement was for a brief time a major sticking point between the U.S. and the EU in negotiations over the Directive, until the Europeans concluded that they didn't want to be the world's privacy policemen and deferred in the first instance to the traditional regulatory authority of the Federal Trade Commission, which had bared its fangs in the Geocities enforcement action.^{xxxiv} The existence of traditional remedies for misrepresentation and detrimental reliance also rebuts critics of TrustE, BBBOnline, and other industry-sponsored privacy initiatives. Such efforts have had significant success in encouraging major websites to post statements of what they do with personally identifiable information. Once companies make such statements to the public, they then become subject to all of the traditional enforcement power of the FTC under Section 5 of the Federal Trade Commission Act, state regulatory analogs, and consumer class-actions. If a company says that it's not going to do something with personal information, and then proceeds to do it, and a consumer relies on the misrepresentation to his or her detriment, that's fraud and the company can be prosecuted as they would be in any other fraudulent transaction.^{xxxv} The need for some showing of actual harm to consumers is a healthy counterweight to the risk of enforcement actions based on technical violations.

Even more powerful sanctions against misuse of personal information come in the form of adverse publicity. Think of just the public privacy "scandals" of recent years – Lotus Marketplace, P-Trak, state DMV sales of driver's license records, Real Networks Real Download software, the DoubleClick / Abacus merger, Geocities, various Microsoft and Netscape browser bugs, Toysmart.com, the outsourcing of site analysis to Coremetrics, and inadvertent violations by TrustE of its own privacy policy. While not one resulted in any significant harm to consumers, the companies involved virtually all took significant hits to their stock prices, and in every case the programs were either withdrawn or promptly fixed.^{xxxvi} Governmental programs deemed to have privacy risks – such as the FBI's "Library Awareness" program or the Department of the Treasury's "Know Your Customer" program – met similar fates. Even privacy advocates concede that "[t]he bad publicity generated by a 'privacy outrage' far outweighs any possible revenue that a company might earn from its customers" and recommend a strategy of "publicize and litigate" in response to potential privacy problems.^{xxxvii}

As I have noted at several points, this reliance on market-based public opinion echoes the argument of John Hart Ely's **Democracy and Distrust**. While we can hypothesize potentially horrible results of the legislative process – such as a law requiring every citizen to have a kidney removed – the best safeguard is not judicial activism in the form of substantive due process (with all of its attendant costs), but rather reliance on the more pedestrian realities of democracy that make such an outcome highly unlikely. Similarly, in the commercial context, the best safeguard against outrageous misconduct or misuse of personal information is the force of public reaction. Certainly the media has not be shy about publicizing even theoretical privacy problems at a rate that far outstrips their real impact on the lives of Americans. As recent privacy stories demonstrate, these consequences (and the inevitable follow-on lawsuits) are often more severe than any regulatory response would be, and come without the burdens, bureaucracy, and market-

distortions that regulation inevitably entails for the many good actors as well as the few bad ones.

There's little evidence that existing laws have proven insufficient in deterring privacy problems, or that there's a need for additional private rights of action. It is simply not that case that there's no justice unless some plaintiff lawyer gets rich. The world of personally identifiable information is rife with "eggshell plaintiffs" who may allege outsize damages from the mis-handling of what would seem trivial information. Even being seen going to the movies with someone during the day may be hugely damaging if it causes you to lose your job or get a divorce. And it's virtually impossible for the recipient of such information to know whether it's sensitive or not. Moreover, since many problems are inadvertent (given the increasingly difficult task of managing information flows), it's unclear whether additional sanctions will further reduce privacy problems, or merely transfer funds from deep corporate pockets to deep trial lawyer ones.

(6) Onward Transfer

The Safe Harbor principles provide that:

"To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.... [FN: It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.]"^{xxxviii}

The FTC seems to support limits on third-part transfers, although fails to acknowledge the Safe Harbor principles' exception for agents, which is essential in the era of the borderless corporation. At minimum, any U.S. regulations will need to carve out contractors, consultants, agents, and vendors in privity with the data recipient and complying with its privacy policies, as described in the Safe Harbor approach. Even with the exception, it will be hard to be a vendor: imagine United Postal Service workers reviewing and complying with dozens of different customer privacy policies for different deliveries. Moreover, many if not most companies have a number of corporate affiliates – formally different corporate entities that are still legally responsible for one another's actions. Prohibitions on inter-affiliate transfers of personal information (as under the Gramm-Leach-Bliley financial industry reforms^{xxxix}) handicap a number of otherwise beneficial exchanges.

We have image of the grocer as different from the barber, and look to personal relationships to govern the handling of information. We don't have those same relationships with the groups of people who make up modern corporations. The recent controversy over Toysmart.com's entry into bankruptcy and its related effort to sell its customer list to another company (which bankrupt companies have done for generations), is thus something of a red herring. So long as information is being used within the "intended scope" of a transaction, the precise identity of those using it shouldn't matter, although material statements about future uses made to those supplying the information should continue to "run with the land" regardless of future transfer.

(7) Data Integrity

For their final component, Data Integrity, the Safe Harbor principles provide that

"Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current. Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current."^{x1}

Again, the goal is unexceptionable, but "the devil is in the details." What is meant by "reasonable steps", and what degree of contact is required? Does this rule apply to downstream recipients of data? If so, for how long? Does it matter whether the information is "sensitive" or not? Filling in these blanks is necessary to give any meaningful sense of the costs of such a requirement.

ⁱ **Privacy Online Report** at iii.

ⁱⁱ U.S. Department of Commerce, **Safe Harbor Privacy Principles** (July 21, 2000) <<http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm>> (hereafter "**Safe Harbor Principles**").

ⁱⁱⁱ **Privacy Online Report** at 24-28; **Privacy Online Report – Leary Concurrence and Dissent** at 2-4.

^{iv} **Privacy Online Report** at 22.

^v **Privacy Online Report** at 24.

^{vi} **Privacy Online Report – Leary Concurrence and Dissent** at 2.

^{vii} **Privacy Online Report – Leary Concurrence and Dissent** at 3.

^{viii} **Privacy Online Report – Leary Concurrence and Dissent** at 5.

^{ix} **Privacy Online Report** at iii.

^x U.S. Department of Commerce, **Safe Harbor Privacy Principles** (July 21, 2000) <<http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm>> (hereafter "**Safe Harbor Principles**").

^{xi} **Safe Harbor Principles**.

^{xii} **Online Profiling Report – Leary Concurrence and Dissent** at 2.

^{xiii} **Privacy Online Report – Leary Concurrence and Dissent** at 6-7 (citations omitted).

^{xiv} **Privacy Online Report – Swindle Dissent** at 21 (emphasis omitted).

^{xv} Exhibit B to Open Letter of Ambassador David L. Aaron, Nov. 15, 1999; posted at <<http://www.ita.doc.gov/ecom>>.

^{xvi} **Privacy Online** at 6 n.16.

-
- ^{xvii} **Privacy Online** at 7 n.19.
- ^{xviii} **Privacy in the Information Age** at 117-18.
- ^{xix} **Privacy Online Report** at iii.
- ^{xx} **Safe Harbor Principles.**
- ^{xxi} **Advisory Committee Report.**
- ^{xxii} **Privacy Online Report** at 31.
- ^{xxiii} **Privacy Online Report – Leary Concurrence and Dissent** at 6.
- ^{xxiv} Final Report of the FTC Advisory Committee on Online Access and Security—Concurring Statement of Stewart Baker <<http://www.ftc.gov/acoas/papers/finalreport.htm>> (hereafter “**Advisory Committee Report – Baker Concurrence**”) (The Advisory Committee “heard estimates from Web companies that less than one percent of customers who are offered access actually take advantage of the offer.”)
- ^{xxv} 6 U.S.C. Sections 601-22.
- ^{xxvi} U.S. Department of Commerce, Safe Harbor Privacy Principles – Frequently Asked Question #8, Question / Answer #1, <<http://www.ita.doc.gov/td/ecom/FAQ8AccessFINAL.htm>>
- ^{xxvii} U.S. Department of Commerce, Safe Harbor Privacy Principles – Frequently Asked Question #8, Question / Answer #1, <<http://www.ita.doc.gov/td/ecom/FAQ8AccessFINAL.htm>>
- ^{xxviii} U.S. Department of Commerce, Safe Harbor Privacy Principles – Frequently Asked Question #8, Question / Answer #4, <<http://www.ita.doc.gov/td/ecom/FAQ8AccessFINAL.htm>>
- ^{xxix} **Privacy Online Report** at iii.
- ^{xxx} **Safe Harbor Principles.**
- ^{xxxi} **Advisory Committee Report – Baker Concurrence.**
- ^{xxxii} “U.S. Security Scare: Dumb and Dumber”, *ecommercetimes.com*, Sep’t 14, 2000
- ^{xxxiii} **Safe Harbor Principles.**
- ^{xxxiv} Geocities complaint available at <http://www.ftc.gov/os/1998/9808/geo-cmpl.htm>; Geocities consent decree available at <http://www.ftc.gov/os/1998/9808/geo-ord.htm>.
- ^{xxxv} The FTC has filed an increasing number of actions against companies and individuals to halt fraud on the Internet. See Ann Bartow, *Learning Law in Cyberspace* n.5 (July 31, 1999), available at <<http://www.cyberspace.org/bartow/index.html>>.
- ^{xxxvi} See generally, “None of Your Business,” **Business Week**, June 26, 2000 at 78 (reviewing business costs of privacy problems, including reduced stock price, lawsuits, and adverse media stories).
- ^{xxxvii} **Database Nation** at 172.
- ^{xxxviii} **Safe Harbor Privacy Principles.**
- ^{xxxix} Pub. L. 106-102.
- ^{xl} **Safe Harbor Privacy Principles.**