

[Submitted by email: privacynoi2010@ntia.doc.gov]

January 28, 2011

U.S. Department of Commerce
1401 Constitution Avenue, NW., Room 4725
Washington, DC 20230

Re: Comments of Chris Jay Hoofnagle on *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Docket No. 101214614-0614-01, RIN 0660-XA22

Dear Secretary Locke:

Thank you for releasing *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*. I respectfully submit the following comments on the Green Paper.

1. d. Should baseline commercial data privacy legislation include a private right of action?

In considering this issue, please note that the options for a private right of action are not binary. Private rights of action could be triggered only where a company fails to honor a safe harbor, or some other condition of responsible use of personal information. The Department may also consider flexible caps on damages, as are contained in the CAN-SPAM Act, which explicitly gives courts discretion to reduce damage awards, and is designed to avoid annihilation liability.

Class action liability is daunting, but it is also important to recognize that courts never impose the 9 and 10-figure damages that are theoretically possible under privacy statutes. Even if they did, the Court's new attention to the substantive due process issues involved in such large damage



awards could curtail these damages and make them proportional to the harm proved in the case.

It is also important to consider that without private rights of action, companies may find it efficient to engage in fraud or invade privacy. The politics of enforcement in recent years has led to a landscape where the government may not be able to fine companies enough for harm to the public. For instance, the Toyota car company was recently fined \$16.4 million by the Department of Transportation, the largest fine that the agency can levy under the law for concealing information about recalls.¹ It is estimated that Toyota saved \$100 million through pursuing a limited recall strategy.

Similarly, there is lack of satisfaction in the recent government actions against Goldman Sachs. While the group settled a SEC case for \$550 million, the New York Times recently opined that the fine was, “chump change compared with Goldman’s bonus pool, and less even than Goldman’s depressed second-quarter profits.”²

In some cases, even very large government fines may not conform behavior to the law. The US government fined Pfizer a staggering \$2.3 billion in 2009 for illegal marketing of pharmaceutical drugs.³ It was the company’s fourth settlement with the government since 2003. With annual revenues of almost \$56 billion,⁴ the fine could be seen as a cost of doing business to Pfizer.

Adding a private right of action diversifies enforcement resources, and could address the problem of agency capture or indifference to consumer problems.

¹ Micheline Maynard, *U.S. Is Seeking a Fine of \$16.4 Million Against Toyota*, THE NEW YORK TIMES, April 5, 2010, <http://www.nytimes.com/2010/04/06/business/06toyota.html>.

² The New York Times, *Goldman’s Go-Round*, THE NEW YORK TIMES, July 20, 2010, http://www.nytimes.com/2010/07/21/opinion/21wed1.html?_r=1&ref=opinion.

³ Gardiner Harris, *Pfizer Pays \$2.3 Billion to Settle Marketing Case*, THE NEW YORK TIMES, September 3, 2009, <http://www.nytimes.com/2009/09/03/business/03health.html>.

⁴ New York Times Analysis Tools, Pfizer, Inc., available at <http://markets.on.nytimes.com/research/stocks/fundamentals/fundamentals.asp?symbol=PFE>

2. e. Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?

A machine-readable format would make it more difficult for privacy policies to feature vague and conflicting terms around key issues.⁵ One reason P3P failed is that lawyers did not want to state in a binary fashion whether a company shares personal information—they preferred serpentine language that made salient, up-front statements (“We will not share information...”) that were defanged by exceptions later on the page. For this reason, experienced privacy policy readers start from the bottom up when evaluating a privacy policy.

A machine-readable format would also assist in policing terms. Consider the Anntaylor.com example at footnote 5—the company uses the term “marketing partners,” which suggests that Ann Taylor only shares with businesses with which it is in a joint venture. Other companies routinely use euphemisms such as “family of companies,” “sister companies,” and even “affiliates” to mean arms-length transactions to sell personal information. A machine-readable statement would include definitions painting a clear line between first and third party sharing.

2. j. Currently, how common are purpose specification clauses in commercial privacy policies?

One way to consider whether the market is protecting consumers adequately is to compare business-to-business agreements with the terms business offer to consumers.

Interestingly, purpose specification clauses are ubiquitous in business-to-business contracts for the sale of personal information. Business to business agreements routinely incorporate fair information practices (including use specification, use limitations, security duties, openness, and

⁵ For instance, this type of statement, from Anntaylor.com, would be impossible to foist upon the user in a machine-readable format: “To respect your privacy, Ann Taylor will not sell or rent the personal information you provide to us online to any third party... In addition, Ann Taylor may share information that our clients provide with specially chosen marketing partners...”

accountability), they are clearly written, and they contain active verbs and certain restrictions on data use, in stark contrast to privacy policies.

For instance, in one B2B contract I found, buyers of personal data assume a duty of confidentiality to the seller, meaning that the buyer cannot reveal the provenance or content of data purchased. This highlights a fundamental misunderstanding among consumers. Consumers think that they enjoy a duty of confidentiality with businesses they frequent. Alan Westin has found repeatedly that about half of Americans believe that, “Most businesses handle the personal information they collect about consumers in a proper and confidential way.” In fact, confidentiality agreements may be used to enable the sale of data so that it will breach the sales contract if the buyer tells the data subject about it.

While many privacy policies contain slippery language concerning sale of personal information to third parties, B2B contracts prohibit it with certainty. One contract specifies: “Client shall not sell, rent or otherwise provide the Licensed Data to any third party.”

Retention of personal information is a contentious issue, and some actors in the debate are vigorously opposing requirements to delete personal data. However, in these B2B contracts, data is required to be destroyed soon after it is used.

Finally, the accountability gulf between the B2B and B2C worlds is vast. Many companies have lobbied to prevent meaningful accountability provisions for consumers. Not so in the B2B world. These contracts, among other things, give the data seller the ability to audit the buyer, they make the buyer fully liable for acts of service providers, require notice to the seller of a security breach (even when the data are not sensitive identifiers normally subject to such duties), and require the buyer to pay for any costs associated with a security breach. One even requires buyers of data to give the seller an express right to sue service providers hired by the buyer for violations of the contract.

Basic economic theory would explain the chasm between B2B contracts and B2C privacy policies—consumers are unaware of these uses of information, they think law protects against them, they do not have the

bargaining power to negotiate changes, and no individual user has the economic motivation to negotiate these changes.

As part of its consideration of fair information practices, the Department should explore enhancement⁶ more deeply. Enhancement is the practice of linking more information about consumers to an existing database. A recent case explored this practice at Williams-Sonoma: “After acquiring this information [zip code from Jessica Pineda at the register], the Store used customized computer software to perform reverse searches from databases that contain millions of names, e-mail addresses, residential telephone numbers and residential addresses, and are indexed in a manner that resembles a reverse telephone book. The Store's software then matched Pineda's now-known name, zip code or other personal information with her previously unknown address, thereby giving the Store access to her name and address.”⁷

The Department should closely examine enhancement, as it contravenes transparency, trust, and fairness principles. The standard (uninformed) self-help argument in this field is: if you don't want your information sold, don't give it out. But enhancement obviates many attempts to protect privacy through selective revelation, robbing the individual of the ability to “entrust” data with a limited number of companies. It tricks the individual into thinking information revelation is required and/or harmless, so that the company can opaquely identify or learn more about the consumer.

⁶ We asked Californians in 2007 about enhancement: “If a website has a privacy policy, it means that the site cannot buy information about you from other sources to analyze your online activities.” Forty-two percent answered true incorrectly, 45 percent correctly answered false, and 12 percent answered don't know. CJ Hoofnagle & J King, *What Californians Understand about Privacy Online*, SSRN ELIBRARY (2008), <http://ssrn.com/paper=1262130>. (N=377)

⁷ *Pineda v. Williams-Sonoma Stores Inc.*, Cal. Ct. App., 4th Dist., No. D054355, certified for publication 10/23/09.

Recommendation 5. The FTC should remain the lead consumer privacy enforcement agency for the U.S. Government.

The narrative of the Green Paper suggests that the FTC should have the role of enforcer, given its expertise in the matter. This narrative is complicated by these facts:

- **The FTC lacks civil penalty enforcement.**⁸ This stands in stark contrast to other nations. All European Union countries have civil penalty enforcement. This civil penalty authority ranges from “€18,900 (\$26,657) in Austria to a high of €600,000 or \$869,292 in Spain...”⁹
- **The FTC has curtailed its own authority, in ways that hamper effective enforcement of privacy rules.** For instance, over the past decade, the FTC has followed a “harm-based” approach as a voluntary constraint on its ability to bring privacy cases.¹⁰ There was no empirical support for the idea that consumers preferred this policy option. And, the FTCA clearly does not require harm. Its text does not mention harm, in fact, the very idea of “deception” is not even defined by the FTCA.¹¹

The harm-based approach was built upon an earlier voluntary limitation of the agency’s power. The 1983 statement¹² drafted by the FTC to explain its broad, undefined deception power was recognized at the time as a political power grab, from the FTC

⁸ 15 USC § 45(m)(1)(A).

⁹ Ali Qassim, New U.K. Penalty Authority Means All EU May Now Fine Data Protection Violators, 9 PVLIR 131, Jan. 25, 2010.

¹⁰ Legislative Hearing on H.R. 5777, The BEST PRACTICES Act, before the Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, 111th Cong. 2nd Sess, Jul. 22, 2010 (testimony of the Federal Trade Commission).

¹¹ 15 USC § 45(a).

¹² FTC, FTC POLICY STATEMENT ON DECEPTION (1983), <http://www.ftc.gov/bcp/policystmt/ad-decept.htm>.

to businesses, by then Regan appointee FTC Chairman James Miller.¹³

- **The FTC believes that it cannot bring cases against aiders and abettors.**¹⁴ This is problematic for the strong privacy enforcement narrative, because modern large scale frauds are dependent on many different actors who are repeat players— adware/spyware vendors, money mules and their managers are key for identity theft rings, and botnets and operators of botnet armies are essential for a wide variety of computer frauds. The use of affiliate marketing generally, while legitimate in certain circumstances, is often a technique to divorce advertisers from less-than-legal schemes to enroll consumers in continuity programs and the like. Aiding and abetting authority makes it possible to do more than simply play whack-a-mole with the advertiser of the week by attacking the infrastructures that act as a force multiplier for fraud.

¹³ “You were directed to provide a definitive neutral analysis of a nearly 50-year old body of consumer protection law that has served as a model for the states and for this nation. We requested a disciplined in-depth review of what decades of case law stand for, and of the nature and amount of evidence and deception considered by the Commission during 50 years of litigation in the public interest. What you delivered is a document that addresses not what the Commission's deception jurisdiction is, but what some now at the agency want it to be.” Letter from Rep. John Dingell, Chairman of the House Oversight Committee, reprinted at 5 Trade Reg. Rep. (CCH) P 50,455, at 56,086 (Oct. 31, 1983), cited in Jack E. Karns, State Regulation of Deceptive Trade Practices under Little FTC Acts: Should Federal Standards Control, 94 Dick. L. Rev. 373 (1989-1990). *See also, Southwest Sunsites, Inc. v. FTC*, 785 F.2d 1431, 1436 (9th Cir. 1986), “Each of the three elements of the new standard...imposes a greater burden of proof on the FTC to show a violation of Section 5. First, the FTC must show probable, not possible, deception (“likely to mislead,” not “tendency and capacity to mislead”). Second, the FTC must show potential deception of “consumers acting reasonably in the circumstances,” not just any consumers. Third, the new standard considers as material only deceptions that are likely to cause injury to a reasonable relying consumer, whereas the old standard reached deceptions that a consumer might have considered important, whether or not there was reliance.”)

¹⁴ Hearings on the Federal Trade Commission Reauthorization Act of 2008, before the Senate Committee on Commerce, Science, and Transportation, 110 Cong. 2nd Sess., Apr. 8, 2008 (Statement of Chairman Jonathan Leibowitz).

- **The FTC’s staffing remains at 1960s levels.** The FTC is responsible for policing a vast section of the US economy. The agency has some responsibility for over 40 laws now. It shoulders this burden with about 1,200 employees. This is down from its peak of about 1,750 employees in the late 1970s. It is simply not possible for one division within one agency to police the broad spectrum of privacy problems that exist.
- **If the FTC is too aggressive, it may suffer from blowback.** Historically, the FTC has been “rewarded” for its work by threats from Congress. The meatpackers, baby-blanket manufacturers, cigarette companies, and advertisers have all played a part in threatening the agency’s powers (and very existence). Fallout from the KidVid proceeding caused Congress to stop funding for the agency, and Congress even banned it from taking enforcement actions in the advertising space for two years. As a result of this, the FTC takes only safe cases. In fact, every case it has pursued has been settled by the target company.
- **The FTC may have allowed “efficient” violations of privacy rules.** For instance, in the agency’s Adinteractive case, the company settled with the FTC and agreed to pay \$650,000 in civil penalties for alleged deceptive advertising practices, when the company reported annual revenues exceeding \$115 million.¹⁵ Similarly, in the DirectRevenue case, the FTC settled

¹⁵ “Whether or not the \$650,000 penalty Adteractive agreed to pay is harsh enough to deter similar violations also is up for debate. Of the five commissioners voting on the settlement decision, one dissented on grounds that the civil penalty is “inadequate.” In his dissenting statement, Commissioner Jon Leibowitz referenced Adteractive’s reported annual revenues of over \$115 million, citing a 2005 San Francisco Business Times article. Industry observers agree the firm, founded in 2000, was making around \$100 million annually by 2005, and a former employee told ClickZ News last month the company was valued at more than \$400 million when business was booming.” Kate Kaye, FTC Settlement with Adteractive Leaves Unanswered Questions for Troubled Firm, ClickZ News, Nov. 29, 2007, available at <http://www.clickz.com/3627728>.

for \$1.5 million for a business practice that gained the company \$20 million in investment revenue.¹⁶

- **Taken together, these factors limit the FTC’s pressure against companies in cases it labels as “privacy initiatives.”** Andrew Serwin, an authority on privacy litigation, has observed, “...the FTC does not have unlimited resources, privacy is not its only responsibility, and the actual number of enforcement actions is not as high as one might guess.”¹⁷ The FTC has obtained 8-figure damage settlements in only two privacy initiative cases—ChoicePoint (\$15M) and LifeLock (\$11M). In the agency’s other 23 privacy initiative cases, it has levied about \$7M in fines. Most cases involving fines are those where the FTC has invoked a sector-specific statute empowering the agency to levy a civil penalty. For instance, the agency obtained \$1M settlements against Sony BMG and Xanga for violations of the Children’s Online Privacy Protection Act. ValueClick paid \$2.9M for violations of the spam law. In the remaining 31 cases—the bulk of the FTC’s privacy initiatives where no civil penalties were obtained in settlement—the agency relied upon two tools to punish violators of privacy: long periods of oversight and the reputational damage of a settlement agreement.

For the Department’s narrative to hold, the Green Paper needs to acknowledge these limits and alter its approach to buttress the FTC. In recent years, Chairman Leibowitz has petitioned Congress to address the APA rulemaking issue and aiding and abetting authority. The Department of Commerce should support these initiatives in order to bolster its narrative surrounding FTC enforcement.

¹⁶ Jason Lee Miller, DirectRevenue Slapped (Lightly) By FTC, Feb. 21, 2007, available at <http://www.webpronews.com/topnews/2007/02/21/directrevenue-slapped-lightly-by-ftc>.

¹⁷ Andrew Service, Poised on the Precipice: A Critical Examination of Privacy Litigation, 25 Santa Clara Computer & High Tech. L.J. 883 (April 2009).

Critically, the FTC needs a constituency—it needs a base of support among industry so that narrow business interests cannot call for the agency’s neutering or decapitation whenever the FTC is aggressive. Thus, the Department should consider whether the very activities it proposes to do should be done instead by the FTC. Industry must be invested in the FTC or it may pursue a capture strategy at Commerce to influence the substantive rules and attempt to limit the FTC’s resources, leadership competence, and authority to reduce enforcement.

8. Are there lessons from the sector-specific commercial data privacy laws—their development, their contents, or their enforcement—that could inform general U.S. Commercial data privacy policy?

In my summary of US privacy laws for the European Commission, I document how companies engage in regulatory arbitrage through business practices that evade the substantive requirements of a sector-specific privacy law, while collecting the very information that the law seeks to protect.¹⁸ The sectoral system has created a culture where many businesses build their systems just outside a statute, use the same data regulated by the statute, and even sell it to the actors that the statute anticipates regulating. One such example is the commercial data broker. These companies sell data very similar to a credit report, to entities that typically buy credit reports, for purposes very close to credit reporting purposes, but nonetheless, the activity remains outside the FCRA.

The discussion above relates to recommendation 3, because commercial data brokers did organize to create a code of conduct. It was called the IRSG (to see what happened to it, visit irsg.org). The FTC, in reviewing the IRSG’s provisions, noted the very risks that came to fruition in the ChoicePoint data breach (the problem of malicious insiders). Privacy advocates pointed out the IRSG’s laughable provisions, including the problem that it greenlighted the sale of data basically to anyone, except the “general public,” which apparently meant only individuals too incompetent

¹⁸ Chris Jay Hoofnagle, *New Challenges to Data Protection Study - Country Report: United States*, SSRN ELIBRARY, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1639161.

to get a business license. Non-IRSG member companies soon emerged, and sold data to the “general public” anyway. IRSG created an illusory opt out right, one that companies complied with by simply stating that the consumer had no right to opt out,¹⁹ because the data broker did not engage in any practices subject to the opt out provisions. Soon after the passage of GLBA, the IRSG stopped functioning, making the promises of auditing and enforcement illusory too.

The history of the Network Advertising Initiative is similarly dismal. The principles that it proposed in 2000 cannot even be found on its own website.²⁰ One would hope that a self-regulatory program could at least maintain an archive of its own documents. IRSG failed at this too.

The NAI opt out only prevents members from targeting advertising based upon tracking, but it still allows tracking. Thus opting out creates a worst case scenario outcome: the user is still tracked but does not enjoy the putative benefit of targeted advertising.

These self-regulatory approaches were very bad for privacy. In the absence of substantive privacy law, commercial data brokers created the very citizen databases that the Privacy Act of 1974 sought to prevent. The government can simply buy data on its citizens now instead of collecting it directly. Citizens have no way to prevent this short of living “off the grid.” Similarly, non-NAI member network advertisers have multiplied, developed more sophisticated methods to track individuals, and engaged in the very behaviors that NAI promised it would prevent, such as the merging of data collection online and off.

What lessons can be learned about this? Self-regulatory groups in the privacy field often form in reaction to the threat of regulation. They create protections that largely affirm their current and prospective business practices. The consumer rights created are narrow. They do not update their standards in response to changes in the marketplace, until the regulatory spotlight returns. Nor do they address new actors that raise

¹⁹ See <https://www.locateplus.com/privacy.asp>

²⁰ The FTC has helpfully archived it here: www.ftc.gov/opa/2000/07/onlineprofiling.shtml

similar concerns but fall outside of the self-regulatory regime. Promises to audit and enforce are often empty. Increasingly, these self-regulatory efforts lack moral force, in part because troubling critiques of them go unaddressed or unanswered.²¹

How could the Department address this? The Framework must endeavor to create self-regulatory systems with much stronger incentives to police the industry. The Department should consider:

- Is it adequately broad to cover the harms posed by the system?
- Is it adequately strong so that consumers are given real rights and choices?
- Does it have incentives for oversight to cause regular review and update in light of new technologies and risks?
- Is it specific enough to clearly delineate between compliant and non-compliant actors?
- Are the audits proposed meaningful, and publicly available?
- Is it powerful enough to discipline its own members?
- Is it powerful enough to broaden its scope when new actors emerge that implicate the same concerns yet fall outside the strict definitions of the program?
- Does the system identify benchmarks which if not met, will trigger a review of the safe harbor?

Respectfully submitted,

/s

Chris Jay Hoofnagle

Attachments:

New Challenges to Data Protection Study - Country Report: United States (January 20, 2010). European Commission Directorate-General Justice,

²¹ See, e.g. PAM DIXON, THE NAI: FAILING AT CONSUMER PROTECTION AND AT SELF-REGULATION, http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf and Chris Connolly, The US Safe Harbor - Fact or Fiction?, Galexia (2008)

Freedom and Security Report, May 2010 . Available at SSRN:
<http://ssrn.com/abstract=1639161>

Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing, Nov. 30, 2010

Chris Connolly, The US Safe Harbor - Fact or Fiction?, Galexia (2008)

**Consumer Protection in Cloud Computing Services:
Recommendations for Best Practices from a
Consumer Federation of America
Retreat on Cloud Computing**

November 30, 2010

Consumer Protection in Cloud Computing Services

Introduction	3
Summary of Recommended Best Practices.....	5
Background	6
Consumer Protection Challenges.....	9
Consumer Concerns About Data Use.....	9
Law Enforcement Access	9
Lock-in	10
Data Security	10
Secondary Uses of User Data	12
Fairness in Terms of Service.....	12
Massive Storage and Massive Failure	13
Jurisdiction	13
The Role of Transparency	14
Consensus Best Practices for Cloud Computing Services	15
Law Enforcement Access to Data	15
Secondary Use.....	16
Portability and Interoperability	17
Data Security	18
“Free” Services	18
Deletion.....	19
Transparency.....	20
Conclusion.....	22
Appendix A: Best Practices in Disclosure for Business-to-Consumer Services.....	23
Appendix B: Sample Disclosure.....	25
Appendix C: Cloud Computing Retreat Participants.....	26

Consumer Protection in Cloud Computing Services

Introduction

Consumers, businesses and government agencies increasingly are storing data and using services “in the cloud.” This has profound implications for consumer protection. Consumers are entrusting family photos, documents, and personal information to others, in an environment where expectations, best practices, and even the law are unclear. Businesses may outsource processes to the cloud without fully contemplating the implications for their customers’ privacy. The growing use of the cloud creates new challenges for consumer protection and privacy, but it also intensifies problems that have long existed.

The Pew Internet and American Life Project identified a range of consumer benefits from cloud services. Consumers have already widely adopted cloud services, but they are not always aware of what a cloud-based service actually is, or the wider implications of storing data in the cloud. For instance, storing information in the cloud creates rich transactional data that may be monitored by service providers or law enforcement. When cloud services are identified to them, consumers say that they use these services because they are convenient, because they can access data from whatever computer they are using, because they are less likely to lose data in the event of a computer failure, and because cloud services make it easier to share data.¹

Consumers can benefit in other ways as well. For example, cloud services can free consumers from the tedious task of setting-up or maintaining IT resources – allowing them to focus solely on whatever task the IT platform enables them to accomplish. The cloud is likely to have a democratizing effect on security, giving access to new features too complex for many users to deploy themselves. New efficiencies inherent in the cloud model will allow businesses to start small and quickly provision

¹ John Horrigan, *Use of Cloud Computing Applications and Services*, Pew Research Center’s Internet & American Life Project, <http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx>

more resources as needed, resulting in savings and fewer service outages.²

Government agencies may also be able to save taxpayer money by using cloud computing services.

Cloud computing itself is difficult to define, but it would be unwise to allow that difficulty to impede efforts to address consumer protection and privacy problems.

Many of the challenges cloud computing creates or intensifies center around control over information. Practically speaking, the cloud's popularity means that more and more information is vested among an array of companies that might not even be known by or have a direct relationship with the consumer. For instance, consumers may sign-up for a web service that lets them easily share photos with friends (direct relationship) – but the photo sharing service, in turn, may employ a cloud service to provide flexible storage capacity (indirect relationship). These providers must have processes and practices in place to ensure data integrity, availability, and security.

Transferring control of data can result in lower legal barriers against law enforcement and civil litigant access to information. This is especially true in the United States, where the Fourth Amendment to the Constitution protects data on devices in possession of an individual but where such protections are generally lessened if data are transferred to a third-party.

There is also the matter of the cloud provider itself gaining access to stored data. Consumers may perceive cloud services like a storage locker: information is placed online in a vault and only the consumer has the authority and ability to “look” at it. That may be true for some cloud models. But in others, the cloud provider may be opening the locker to view its contents, and even monitoring transactional data to see how those contents are used. Sometimes service providers need to access data to facilitate a customer request or ensure that the service is functioning properly (technical

² Michael Armbrust et al., *Above the Clouds: A Berkeley View of Cloud Computing*, *Electrical Engineering and Computer Sciences*, UC Berkeley, www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf; World Economic Forum, *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation*, 2010, available at <http://www.weforum.org/pdf/ip/ittc/Exploring-the-future-of-cloud-computing.pdf>

justification). In other instances, service providers may scan hosted data for a secondary use that helps fund the provision of the service (business justification). In fact, the provider's business model may depend upon analysis and decision making based upon consumer data.

Unresolved, concerns about cloud computing are likely to prevent widespread adoption of valuable and efficient services. Providers may also face stringent regulatory interventions because of the opaque nature of data security measures and lack of clarity on the actual location of cloud data. These issues led a German Data Protection Authority to conclude recently that cloud providers must locate their services within the European Union, and that personal data should not be placed in cloud services.³

Summary of Recommended Best Practices

This report makes recommendations for best practices for business-to-consumer cloud computing services. Our goal is that these best practices will diffuse deeply into the business community, so that companies considering the outsourcing of customer data to the cloud will also consider them in their decision making:

- **Law Enforcement Access to Data.** Where not prohibited by law, users should receive notice of criminal and civil requests for information.
- **Secondary Uses.** Secondary use must be clearly disclosed and identified as “technical justifications” or “business justifications” for use of data.
- **Portability and Interoperability.** Portability is key for competition in cloud services; cloud service operators should not interfere with interoperability.
- **Data Security.** Cloud service providers must demonstrate operational safeguards and security mechanisms through expert audit and certification.

³ Andrea Schuessler, *EU Data Protection: German State DPA: Non-EU Clouds Off Limits, Personal Data Should Never Be Sent to Cloud*, 9 BNA Privacy & Security Law Report 950, Jun. 28, 2010, citing Cloud Computing and Data Protection, at <https://www.datenschutzzentrum.de/cloud-computing/>

- **“Free” Services.** “Free” services should have the same consumer protection standards as for-fee services.
- **Deletion.** Consumers should be able to delete information they upload to the cloud.
- **Transparency.** Basic information such as such as the level of service provided, the business model of the cloud service provider, what legal protections apply to data, and who to contact if questions arise should be provided. The report includes a model disclosure for this information.

These recommendations emerged from a two-day retreat convened by the nonprofit organization Consumer Federation of America focusing on cloud computing challenges.⁴ The participants in the retreat included persons from consumer and privacy organizations, academia, government, and business, from both the US and Europe. While a few of the participants chose not be included in the list that appears in Appendix C because of legal or other constraints, all were fully engaged in the process and contributed to the outcome. Regarding those who are listed, their listing is not an individual or organizational endorsement of every statement made in the report. The recommended best practices, however, represent the consensus view of the participants on those issues. As noted above, there was consensus that secondary uses should be clearly disclosed, but there was disagreement over whether secondary uses should be left to contract, limited where the consumer is not likely to understand the use, or flatly prohibited.

Background

Cloud computing is difficult to define.⁵ A recent report by the World Privacy Forum describes it as involving “the sharing and storage by users of their own

⁴ This retreat took place at New York University School of Law in New York City on June 20-22, 2010. The reporter for the group and author of this report was Chris Hoofnagle, Senior Fellow at the Berkeley Center for Law & Technology.

⁵ The National Institute of Standards and Technology defines it as, “...a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” This is NIST’s 15th version of this definition.

information on remote servers owned or operated by others and accessed through the Internet or other connections.”⁶ Popular cloud-based consumer services include webmail (such as Gmail and Hotmail), photo sharing sites (such as Flickr), and even social networking sites (such as Facebook and MySpace).

Consumer protection and privacy concerns in cloud computing largely focus upon control over information. That is, the lack of physical control over data entrusted to cloud providers creates potential legal and technical challenges. Retreat participants focused on vesting control of data to another as an organizing principle for these best practices.

Cloud providers themselves are careful to define services as fitting into several categories: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). However, it is unclear whether these distinctions hold in practice (some companies offer packages constituting several or all of these services) or whether consumers honor these distinctions (consider the Gmail user employing the email service to store large files instead of or in addition to communicating with others). Reducing uncertainty in the cloud space may require principles to cover all of these platforms despite their differences.

Both consumer groups⁷ and technology leaders⁸ have called for legal reform to increase the privacy and security guarantees in cloud computing. A thumbnail sketch of the legal landscape elucidates the underlying need for this reform.

U.S. federal privacy law, which has not been updated substantively since 1986, leads to uneven protections for data in the cloud. Data stored on the user’s hard drive is subject to the full protections of the Fourth Amendment, meaning that in most circumstances, the government would need to convince a judge to grant permission to access the data. However, once data are transferred to the cloud, Fourth Amendment

⁶ World Privacy Forum, *Cloud Computing and Privacy*, n.d., available at <http://www.worldprivacyforum.org/cloudprivacy.html>

⁷ Alan Weissberger, *ACLU Northern CA: Cloud Computing – Storm Warnings for Privacy?*, the Viodi View, <http://viodi.com/2009/02/13/aclu-northern-ca-cloud-computing-storm-warning-for-privacy/>

⁸ Microsoft, *Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing*, 2010, www.microsoft.com/presspass/presskits/cloudpolicy/default.aspx

protections may no longer have effect. Under the “third party doctrine,” data knowingly and voluntarily transferred to a third party (such as a cloud service provider) may lose its Fourth Amendment shield. In place of the Fourth Amendment, an outdated and weaker framework of statutory protections takes over. Under this framework, cloud data protections depend upon context.

Robert Gellman summarized the cloud legal landscape in 2009: “Distinctions recognized by ECPA [Electronic Communications Privacy Act of 1986] include electronic mail in transit; electronic mail in storage for less than or more than 180 days; electronic mail in draft; opened vs. unopened electronic mail; electronic communication service; and remote computing service. Case law and scholarly discussions continue to address and debate the proper application of the ECPA’s distinctions to current Internet activities. The courts have struggled in applying ECPA to situations not contemplated by the law’s drafters.”⁹

These distinctions have created increasing uncertainty for both consumer and business users of cloud-provided services. Business models that have evolved since 1986 mix storage and communications services, and many sites enable users to communicate as an incidental offering to some other service. Gellman continues: “The precise characterization of an activity can make a significant difference to the protections afforded under ECPA. For example, if an ‘electronic communications service’ holds a text message in ‘electronic storage’, then law enforcement requires a probable cause warrant to obtain access. If a ‘remote computing service’ stores the same text message on behalf of the subscriber, then law enforcement does not need a warrant, and a subpoena is sufficient. Whether a search engine or social networking site is a remote computing service remains in dispute.”¹⁰

While a consumer-business coalition has organized to reform and update ECPA,¹¹ legislative change moves more slowly than the spread of new services. In the

⁹ Bob Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, 2009, http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

¹⁰ *Id*

¹¹ The Digital Due Process Coalition, available at <http://www.digitaldueprocess.org>

absence of such reform, more certainty is needed to address these barriers to cloud adoption.

Even if new laws are enacted to address cloud computing, it is important to recognize that the US privacy framework is sectoral, meaning that certain industries may not be regulated under a specific privacy law. Thus, the sectoral approach leaves gaps where protections are uneven. Privacy advocates and industry groups alike have called for more comprehensive protections for consumers.

Consumer Protection Challenges

There are a myriad of consumer privacy concerns in cloud computing services. Participants at the two-day workshop identified a range of concerns that could fit into nine categories.

Consumer Concerns about Data Use

A 2008 Pew Internet & American Life Project report¹² elucidated consumers' biggest concerns about cloud services. Ninety percent of respondents surveyed stated that they would be "very concerned" if cloud providers "sold your files to others." Eighty percent would be very concerned if the service "used your photos and other information in marketing campaigns." Sixty-eight percent would be very concerned if information stored in the cloud were used to tailor ads. Sixty-three percent would be very concerned if the cloud provider kept files after the consumer attempted to delete them.

Law Enforcement Access

Law enforcement access looms large for consumers as a concern as well. Forty-nine percent of those surveyed for the Pew report said they would be very concerned if cloud providers "gave law enforcement agencies your files when asked to do so." Some may say, "If you have nothing to hide, you have nothing to fear." But in the cloud

¹² John Horrigan, *Use of Cloud Computing Applications and Services*, Pew Research Center's Internet & American Life Project, <http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx>

context, especially in “public clouds,” transgressive behavior of one consumer can affect others. For instance, if one user employs a shared (or “public”) cloud service to commit a crime, investigators may seize computers or backups that contain the data of the guilty and innocent alike on that shared service. Providers may also be pressured to scan their systems for copyright enforcement or illegal content.

Consumers may not even realize that their data has been moved to the cloud, especially when using new devices such as smartphones. It seems arbitrary for Fourth Amendment protections to hinge upon technical design and service questions that are increasingly complex and not in control of the user.

Lock-in

Other, more subtle challenges exist. For instance, consumers may not understand the lock-in risk until they decide to leave a provider. A consumer might spend many years uploading volumes of information, or otherwise customizing the service. These actions could cause a consumer to be effectively locked to a particular service or provider, threatening competition.

Providers could use proprietary formats or employ subtle technical obstacles to exporting this data in order to capture customers. These could be as simple as requiring consumers wishing to export their data to select each file individually for download. Requiring the consumer to click through page after page of files to accomplish a simple export task could effectively make the service non-portable.

Data Security

Consumers are right to expect that data entrusted to the cloud will be stored securely, meaning that the data will be protected from unauthorized access, be maintained with integrity, and backed up in case of loss. However, in their survey of 31 terms of service contracts for cloud providers, Simon Bradshaw, Christopher Millard, and Ian Walden observed:

A natural concern for Cloud computing customers is that data placed into the provider’s Cloud be secure against loss, be it loss of integrity or availability (resulting, for example, from corruption or deletion) or loss of confidentiality (due perhaps to a security breach

or an unauthorised disclosure). Our survey found however that most providers not only avoided giving undertakings in respect of data integrity but actually disclaimed liability for it.¹³

They continue:

...In effect, a number of providers of consumer-oriented Cloud services appear to disclaim the specific fitness of their services for the purpose(s) for which many customers will have specifically signed up to use them. Some providers...state that data integrity will only be guaranteed where the customer has paid for additional specific backup services.

Since many providers will not create legal assurances for data security and integrity, the consumer must simply trust the service provider.

In the cloud, consumer control of data can be diminished depending on the deployment and service model at issue, and consumers may lack effective mechanisms to determine whether security protections comply with established criteria. Insider threats are more severe, since a single corrupt employee of a cloud provider may be able to access many different accounts and obscure logs of such access.

Further, even if security criteria are disclosed, consumers may not understand what they mean or whether they are adequate, making comparisons impossible. Only a small number of cloud computing users may have the clout, technical capability, and resources to thoroughly evaluate a service provider's security protections. These concerns over security, and the diminished ability of consumer to verify security in the cloud, are key challenges for the adoption of cloud computing.

Security breach notification laws attempt to bridge the gap of consumer awareness of security issues by informing individuals when an unauthorized party obtains certain sensitive information. Such laws create a performance-based security standard that can help consumers and regulators understand whether a company's security implementation is reasonable. However, it is unclear how this approach will work in the cloud, because the scope of security breach notification laws and their

¹³ Simon Bradshaw, Christopher Millard and Ian Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper No. 63/2010, available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374

implementation may lead providers to fail to notify users after a breach. For instance, data may be stored in a jurisdiction not subject to security breach notification, or cloud services may be exempted from breach notification.¹⁴ Cloud providers may argue that their services are “data agnostic,” meaning that the provider does not know specifically what kind of information is stored in an account. According to this reasoning, the cloud provider would not have to issue breach notifications, because it does not know that it possesses sensitive information. This is a dubious argument. It is certainly foreseeable that users will upload personally identifiable information into cloud services, especially when using backup products that mirror the user’s entire hard drive.

Moreover the key issue here is whether the cloud provider knows that there was a breach of security. When breaches occur, the best course of action is to enable users to make their own judgments and take appropriate steps if necessary.

Secondary Uses of User Data

Recall the Pew Internet study finding great concern over marketing uses of data. This is an example of a “secondary use,” the employment of user data for purposes not related to the technical operation of the service. Cloud providers may employ secondary uses of consumer data or transactional information without consumers realizing that those uses are taking place or whether those secondary uses have legal implications. For instance, the scanning of email content in Gmail is a secondary use of communications data. Using email message content to target advertising could erode consumers’ legal rights by diluting their expectations of privacy in the communications.

Fairness in Terms of Service

Terms of service represent another challenge in the cloud. Courts have given legitimacy to one-sided agreements that reflect no bargaining or even the opportunity to bargain. Bradshaw et al. found that many contracts for cloud services were silent on key terms.¹⁵ Worse yet, providers often reserve the right to change terms at will.¹⁶

¹⁴ See e.g. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (and 2009 telecommunications regulations).

¹⁵ See fn. 13 supra.

Important terms can be buried in long user agreements. There is a need for consensus around what terms are important to consumers about a cloud service, and for a prominent disclosure of those important terms, in plain language. This is an area that may benefit from standardization,¹⁷ and the model disclosure in Appendix B attempts to present key terms (that are often not disclosed at all) to consumers in a short notice.

Massive Storage and Massive Failure

Of course, terms change radically when a business fails. One benefit of cloud computing—massive storage—has a potential downside: the problem of massive failure. Thought must go into the possibility that cloud providers will fail well in advance of an adverse event, which might be simply bankruptcy or a natural disaster that affects the provider's infrastructure. Obviously systems have to be backed up, but also, there have to be provisions and sufficient time for consumers to export their data when a cloud provider ends operations.

Jurisdiction

Rules of consumer protection and law enforcement access vary from jurisdiction to jurisdiction. This is a particularly challenging problem with respect to cloud services, because the most efficient design is one that allows data to flow from region to region, or exist in several different regions, without regard to local rules or the lack of them.

On the other hand, jurisdiction may offer opportunities for greater privacy or consumer protection. For instance, one Canadian-based cloud services provider now advertises a service that is based only in Canada, thus reducing the risk that user data

¹⁶ EPIC, Cloud Computing, available at <http://epic.org/privacy/cloudcomputing/>

¹⁷ For example in the UK the importance of improving quality of information under terms and conditions has been recognized by the Financial Services Authority that recently introduced the summary box model in delivering information on financial services to consumers, see Financial Services Authority, Banking Conduct Regulation, Jun. 29, 2010, available at http://www.fsa.gov.uk/Pages/consumerinformation/product_news/banking/banking_conduct_regulation/index.shtml

will be obtained by other governments.¹⁸ Risk is reduced in this approach because users are exposed to the legal framework of only one government, in this case, a government with a strong privacy protection framework established in law.

Just as there are benefits in allowing the business models to develop, thrive or decline in economic models, it is also important to allow legislatures to develop new approaches to address consumer protection as new technologies, policies or business practices emerge.

The Role of Transparency

Transparency is a bedrock approach for consumer protection challenges. It obviously will play a role in assuring consumer and business users of the cloud. However, transparency has to be done well in order to work.

Relevant information must be provided, at the relevant time. Key terms that materially affect the legal and technical status of cloud data must be policed. For instance, a “private cloud” in industry parlance represents a service dedicated to a single entity, rather than multiple users. This has obvious legal and technical implications. But imagine the confusion that could be caused by a provider that decided to call its business “PrivateCloud” without provisioning dedicated service. Thus, this and other key terms in cloud computing must be policed and used only where appropriate, in order to ensure a fair marketplace.

To address the challenge of transparency, we propose best practices in cloud services disclosure for business-to-consumer (B2C) cloud services. We hope that these simple statements will help consumers focus on key legal and technical issues, and prevent providers from obfuscating practices. From a provider perspective, this standardized statement can provide competitive advantage—it will enable comparative analysis, and be especially useful for companies innovating in the privacy and security realms, where it is difficult for consumers to compare service offerings.

¹⁸ CentriLogic, CentriLogic Launches First Canadian-Based Distributed Cloud Computing Service, Apr. 7, 2010, <http://www.centrilogic.com/announcements/newsitem.php?news=19>

Despite all of these challenges, an opportunity exists to manage these risks. These challenges are shared by both average consumers and businesses. It is clear that adoption of cloud services will suffer if uncertainty persists on the issues identified above. Consumer protection in the cloud context clearly is good for both consumers *and* businesses.

Consensus Best Practices for Cloud Computing Services

Participants in the retreat organized by Consumer Federation of America discussed challenges and opportunities for consumers in the cloud computing arena. A consensus developed around the following high-level principles to promote consumer protection, security, and privacy in cloud services. These recommendations go beyond calls for transparency and urge providers to follow baseline practices to foster a climate favorable to consumer and business adoption of cloud services. We hope that businesses that are considering using cloud services will follow these best practices to ensure that their customers' interests in privacy and security are adequately protected.

Law Enforcement Access to Data

A consensus emerged that data stored in the cloud should have the same Fourth Amendment protections as data in possession of an individual. Although providers do not have the power to change the law that applies to cloud services, they can follow certain policies, procedures, and technical design to maximize privacy rights. The group agreed that where service providers are not prohibited by law, they should notify consumers when a law enforcement or civil request has been made for their information.

Legal protections sometimes are justified based upon the employment of technical measures, such as privacy settings. Thus, cloud service providers that make encryption and other privacy-enhancing technologies available to consumers will be at a competitive advantage.¹⁹

¹⁹ However, recent renewed calls for enhanced mechanisms to facilitate law enforcement access to data held by private networks could affect any competitive advantage gained through such technologies. See

Secondary Use

The group could not come to consensus about the appropriate extent of secondary uses in cloud service models. Some argued that secondary uses were not well understood by consumers, and that such uses inherently conflict with a cloud provider's role as information fiduciary. Consumers may conceive of a cloud service as akin to a storage locker—as a rental company that simply rents space that is physically locked by the consumer. A secondary use business model is one where the rental company breaks the lock and periodically peeks at the contents of the locker. Not only that, the rental company may track and record the consumer's comings and goings, how often they open the unit, etc.

Other retreat participants argued that secondary uses might constitute the basis of the bargain for provision of the service. Consumers may be willing to have content or transactional information scanned for advertisements or for analytics in exchange for discounted or free services. Other participants argued that secondary uses should be prohibited altogether.

The group did achieve a clear consensus requiring transparency for secondary uses. Providers should clearly demarcate uses for data that are necessary for operation of the service, "technical justifications," versus "business justifications," that is, uses of personal information that are related to the business model employed by the provider. For instance, monitoring the amount of use a consumer engages in is operationally necessary to address issues such as forecasting the need for more servers or bandwidth. Conversely, accessing content or transactional information for advertising or other marketing activities is a clear business secondary use that is not necessary for technical operation of the service.

Furthermore, when a provider develops new uses of content and transactional information, it should notify the consumer and use an opt-in consent standard before deploying the new use.

e.g., Charlie Savage, *Officials Push to Bolster Law on Wiretapping*, New York Times, Oct. 18, 2010, available at <http://www.nytimes.com/2010/10/19/us/19wiretap.html>

Portability and Interoperability

A consensus emerged that data portability is a key issue to competition and user freedom. The risk of lock-in is a substantial barrier to adoption of cloud services for consumer, business, and government users. Consumers should be able to easily export the information they supply to and generate in the cloud.

This risk of lock-in reaches its zenith in highly-sticky, popular web services, such as Facebook. Consumers spend years enhancing their profiles and building links to friends in environments that do not support portability, thereby creating imposing switching costs for individuals who wish to change to different services. These sites leverage network effects to become popular, but once they have obtained broad adoption, stickiness and a lack of portability reduces competitors' chances of attracting users.

On the other hand, it is precisely this social graph and related services that constitute the "special sauce" of Facebook and similar companies, at least a part of whose success is attributable to innovation and investment. Some argue that it is unfair for consumers to use a free service and also have the option to take the value from that service at will.

A subset of the group argued that nevertheless, competition would be enhanced by the ability of consumers to export all information related to their profiles. This group argued that while services like Facebook have created compelling platforms for interaction, they are fueled by the currency of consumers' personal information and attention. In the case of Facebook and many of its competitors, users are subjected to advertisements. This points to an exchange in value and bolsters the argument that users of services like Facebook should be able to export their data when they desire. On balance, the interests of consumers and competition would be served by the ability to export this information elsewhere.

Data portability may raise nuanced privacy problems if not implemented carefully. James Grimmelman, in his article *Saving Facebook*, elucidates risks of unintended privacy harms: if the exported data are moved to a service with different norms or privacy rules, it could result in consumers pulling information about others

into less-protected spaces.²⁰ If, for instance, a consumer set restrictive sharing preferences in Facebook, should that consumer's friends be able to export the data to another service that is less restrictive?

Interoperability is a related and important issue to portability. Consumers and businesses alike will benefit from the employment of standard data formats that lower switching costs and prevent lock-in. A consensus emerged that providers should not affirmatively interfere with interoperability.

Data Security

Consumer control is a particular challenge in the cloud. While consumers may experience an effective increase in security protections through cloud services, they also may lose the ability to make smart security decisions based on how they—or trusted experts—evaluate the risks of using a particular service. Thus, it is particularly important that cloud providers work to demonstrate operational safeguards and verify trusted security mechanisms in a transparent manner—without jeopardizing the security of the wider community through complete disclosure.

Transparency is so important in this realm that it is our consensus view that cloud providers should make their systems available for analysis by outside security experts. This could take the form of expert audit, which would result in the conferral of an industry-recognized certification. Such certifications (e.g., ISO-27001/2) demonstrate to both active and prospective customers alike that the provider is taking necessary steps to protect personal data.

“Free” Services

Our consensus view holds that “free” services should be subject to the same rules as traditional for-pay services. It is said, “Consumers get what they pay for,” but in the case of “free” services, *consumers are paying*. Providers operating “free” services profit through the currency of personal information instead of direct payment.

²⁰ 94 Iowa Law Review 1137, 2009, available at http://works.bepress.com/james_grimmelman/20

Creating a level playing field for for-pay and free services will enhance competition. Without parity, “free” services will compete by cutting corners rather than providing quality services; this will actually dilute best practices, causing for-pay services to join free alternatives in a race to the bottom.

Deletion

Our consensus view is that consumers should have the right to delete the data they upload to the cloud. There was some disagreement surrounding the extent to which consumers should have the ability to delete data. It seems intuitive that consumers should be able to delete the data they upload to storage and similar services. However, a consensus did not emerge surrounding data that is generated in the cloud itself. For instance, a consumer may tag someone else’s photos, write on the “walls” of social networking sites, and the like. Some thought that such material would not be subject to a deletion option, while others thought that deletion should be more expansive. User deletion is a complex issue and there is still much to resolve. It may be costly and complex, for instance, for providers to delete data in backup systems. Furthermore, the volumes of transactional data generated in the cloud presents policy and technical challenges for deletion.

We are aware that sometimes, consumers state that they wish to delete their cloud data, and later regret the decision, often asking the provider to somehow recover the material. An interesting approach to this problem is found in a Norwegian best practices standard concerning cloud storage of photographs.²¹ Under that standard, customer files and metadata are quarantined for a period before being actually deleted. This makes the data unavailable to both the consumer and the cloud provider, for a specified period of time, unless the consumer reactivates the account.

²¹ Norwegian Consumer Council, New standard for secure online photo storage, available at http://forbrukerportalen.no/Artikler/2010/standard_for_secure_online_photo_storage

Transparency

Transparency is a critical aspect of consumer protection, but by itself, it may fail to achieve results in line with reasonable consumer expectations. In cloud services as with many other technical products, subtle design decisions can have profound implications for consumers, and consumers often do not perceive these issues until they encounter a problem.

Recall the discussion above concerning portability. At enrollment, consumers probably are not thinking about the idea that someday, they may have to cancel their service and wish to remove data from the cloud. A clear disclosure on this important subject made available when the individual is comparing services, could sensitize the consumer to this concern, and cause some consideration of the importance of portability to that particular user.

We think that clear disclosure of key terms will prepare consumers to think through the implications of adopting cloud services, and make better decisions. We also believe that a model disclosure will enhance competition in this space, as its information-forcing value is likely to cause providers to end marginal practices and to highlight meaningful ways in which services are distinguished from others.

The model disclosure in Appendix A focuses on several key issues:

- What is the cloud service provider's business model? Bradshaw et al. found that the business model was key in influencing the terms on which service is offered.²² It thus must be completely clear how the cloud service provider intends to monetize its product. It is not clear at all that consumers understand that some providers intend to use data uploaded to the cloud or transactional data for secondary purposes. Consumers may see that web services are advertising-supported, but many may not understand the extent to which data they provide is used to tailor marketing.

²² See fn. 13 supra.

- What entity actually provides the cloud service? In order to evaluate competitors, the actual service provider's identity is critical information for consumers and business users concerned about possibly providing data to a competitor or to a government with adverse interests.
- Is consumer content or transactional information shared? If so, with whom? Recall that information sharing is a key consumer concern according to the Pew Internet study. Far too many privacy policies cryptically discuss information sharing. Some use the word "partner" to mean third party. Some muddy the waters by making speculative statements about sharing: "We may, from time to time, share information with carefully chosen marketing partners..."
- Is consumer content or transaction data used for purposes not required for the technical operation of the service? A key consumer concern is secondary uses of information unrelated to the technical operation of the service. These uses need to be prominently disclosed in order for the consumer to understand the basis of the bargain.
- Is the provided service a private or public cloud? Whether data are stored on a shared resource or a dedicated one is critical for practical privacy and security concerns.
- What data can the consumer export and in what format? Portability is a key issue, and practically, the formats in which one can export data are important for determining whether a service is compatible with the consumer's existing software.
- Will consumers be notified of security breaches? Security breach notification laws have broad application, but do not always require notice to consumers in the cloud computing context. For instance, some providers are "data agnostic," meaning that they do not claim to know whether a consumer's account contains trigger information for security breach notification laws. Consumers may falsely assume that providers

are required to notify them of breaches; policies surrounding notification should be made clear.

- Where are data stored and what law governs the privacy and security aspects of the cloud provider's services? Generally speaking, consumers are not aware of where a service stores their data or what laws protect (or do not protect) data uploaded to the cloud. A short disclosure of which laws are applicable will guide users in choosing services.
- What procedures are followed when closing accounts? Consumers need to know how services will handle problems such as non-payment and the potential bankruptcy or massive failure of a service provider.
- Who is responsible for consumer and privacy issues and what is their contact information? Including accurate contact information for the individual responsible for consumer privacy and security concerns is extremely helpful for when consumers have questions or when problems arise. This information should include not only company specific resources, but consumer protection and regulatory resources for dealing with complaints when a situation cannot be resolved with the company.

Conclusion

It is our goal that these best practices for business-to-consumer services will reduce uncertainty and promote competition in cloud computing. We believe that consumers, businesses, and governments will benefit from more transparency, and a commitment to the consensus values identified in this document

Appendix A: Best Practices in Disclosure for Business-to-Consumer Services

**Answers to the questions provided are illustrative.*

1. What is the cloud service provider's business model?
 - a. "We charge consumers a fee for this service."
 - b. "We serve advertising based upon consumers' interests in exchange for the service"
 - c. "We analyze consumers' information in order to serve advertising based upon their interests"
2. What entity actually provides the cloud service?
 - a. "We provide it directly"
 - b. "We provide it directly, and use the following subcontractors..."
 - c. "We subcontract all services to..."
3. Is consumer content or transactional data shared? If so, with whom? What choice mechanisms are in place?
 - a. "No"
 - b. "Yes, we share information with affiliates, and you can opt out by X"
 - c. "Yes, we share information with third parties, and you can opt out by X"
4. Is consumer content or transaction data used for purposes not required for the technical operation of the service?
 - a. "No"
 - b. "Yes, we use content/transaction data to target advertisements"
5. Is the provided service a private or public cloud?
 - a. Private cloud: the service is provided for a single entity
 - b. Public cloud: many consumers may be using the same service
6. What data can the consumer export and in what format?
 - a. The consumer can export all data that the user provides in standard formats, including csv, txt, xls.
 - b. The consumer can export data only in proprietary formats
7. Will users be notified of security breaches?
 - a. Yes, according to the law of [jurisdiction]
 - b. No
8. Will the consumer be promptly notified if there is a law enforcement or civil request for data about the consumer?
 - a. Yes, if we are legally able to notify users
 - b. No
9. In what jurisdiction are the data stored?
 - a. [list one or more countries]
 - b. [indicate whether user or service has discretion to select storage location]
10. What jurisdictions' laws govern the privacy and security aspects of the cloud providers' services, and what is the relevant consumer protection authority?

11. What procedures are followed when closing accounts?
 - a. We will give consumers 30 days of access before closing their accounts for non-payment
 - b. In the event of discontinuance of service, we will give consumers 30 days of access to extract data
12. Who is responsible for consumer and privacy issues and what is their contact information?
 - a. Name responsible employee and provide contact information.

Appendix B: Sample Disclosure

Our Business

We provide services to you for a fee.

We own and operate the equipment for this cloud service.

Your Data

We do not share content or transactional data with third parties.

We only use content and transactional data for purposes required for the technical operation of the service.

You can export data uploaded and generated on this service in standard formats, including csv, txt, and xls.

If possible, we will notify you if another party requests data or information about your use of this service.

Our Cloud

Your service level is a private cloud, meaning that we are using a dedicated infrastructure for your services.

Our cloud operates in the following countries: the USA and Canada.

Our cloud services are governed by the laws of the USA and Canada and by the following regulators:

U.S. Federal Trade Commission
Privacy Commissioner of Canada

Security

If we become aware of a security breach, we will inform you of it consistent with the law of California.

In January 2010, our service was certified as compliant with ISO-27001/2 by our auditor.

Account Termination

In the event of a termination of our services, or nonpayment on your account, we will give you notice and 30 days to export data from our cloud.

Contact Us

Our privacy and security contact is:

Joan A. Privacyofficer
1 Embarcadero Center
San Francisco, CA 94001
(415) 555-1212
privacyofficer@cloudprovider.com

Appendix C: Cloud Computing Retreat Participant List

June 20-22, New York City

Svenn Anderson
Policy Advisor
Norwegian Consumer Council

Beth Givens
Director
Privacy Rights Clearinghouse

John Breyault
Vice President of Public Policy,
Telecommunications and Fraud
National Consumers League

Rick Gordon
Managing Director
Civitas Group

Justin Brookman
Senior Fellow
Center for Democracy and Technology

Susan Grant
Director of Consumer Protection
Consumer Federation of America

Jules Cohen
Director of Online Privacy and Safety
Microsoft

Chris Hoofnagle
Lecturer
University of California Berkeley Center
for Law & Technology²³

Mike Egan
Director of Government Affairs
Microsoft

Brian Huseman
Senior Policy Counsel
Intel

David Fagan
Partner
Covington & Burling LLP

Marzena Kisielowska-Lipman
Senior Policy Advocate
Consumer Focus

Harold Feld
Legal Director
Public Knowledge

Cornelia Kutterer
Senior Manager, Regulatory Policy
Microsoft

Robert Gellman
Privacy Consultant

Falk Luke
Policy Officer, Consumer Rights in the
Digital World
Federation of German Consumer
Organizations

Colin Gilbert
Director
Civitas Group

²³ Affiliation for identification purposes only.

Helen Nissenbaum
Professor, Media, Culture and
Communication
New York University

Marco Pierani
Head of Public Affairs
Altroconsumo

Ira Rubinstein
Senior Fellow
Information Law Institute
New York University School of Law

Linda Sherry
Director, National Priorities
Consumer Action

John Simpson
Consumer Advocate
Consumer Watchdog

Katherine Strandburg
Professor of Law
New York University School of Law

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation

Frank Torres
Consumer Affairs Director
Microsoft



EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

COMPARATIVE STUDY
ON
DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES,
IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS

Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28

COUNTRY STUDIES

(Douwe Korff, Editor)

B.1 – UNITED STATES OF AMERICA

BY

Chris Hoofnagle

Submitted by:



LRDP KANTOR Ltd (Leader)
In association with



Centre for Public Reform

(Final edit – May 2010)

UNITED STATES OF AMERICA

By Chris Hoofnagle

I. Context of information privacy in the United States of America

This memorandum summarizes federal US privacy protections, and compares them to approaches made in the states of California and New Jersey.

The hallmark of the US federal approach to privacy is sectoral regulation. A panoply of statutes now regulates specific types of government and business practices, with no broadly-applicable privacy statute governing data collection, use, or disclosure.¹ The Federal Trade Commission has encouraged self-regulation in a number of sectors, and the development of privacy-enhancing technologies.²

In the US system, consumer protection and privacy³ are primarily left to the states. Like the federal government, states regulate privacy through sector-specific statutes, and through state-based constitutional rights.⁴ State constitutional guarantees can exceed federal protections, and in most sectors, federal statutory protections can be enhanced through complementary state law.⁵ Two States are discussed here: California, which has developed both constitutional rights in privacy, and a very wide array of sector-specific statutes;⁶ and New Jersey, where the courts have consistently expanded protections for privacy beyond federal guarantees based upon that State's constitution.

The many different actors in privacy along with the gaps created by a sectoral model prevents the country's privacy framework from fitting neatly into a standard data protection paradigm. There are no cohesive, core concepts to US privacy law. In some contexts, individuals may enjoy a broad set of fair information practices in data, in others, rights may only be based in self-regulatory norms. Sometimes this determination hinges upon the technology used to collect personal information. In other contexts, it depends on the role the information collector plays.

The reader must bear in mind when reviewing this report that the US approach is incoherent, sectorally-based, and that legislative protections are largely reactive, driven by outrage at particular, narrow practices. Still, several innovations from the US approach deserve attention. First, increasingly, privacy statutes create evolving standards of care, thus encouraging innovation for handling of data and avoiding the reification that can result from

¹ Paul Schwartz, Preemption and Privacy, 118 Yale L. J. 902 (2009).

² Federal Trade Commission, Protecting Consumers in the Next Tech-ade: A Report by the Staff of the Federal Trade Commission, Mar. 2008, available at <http://www.ftc.gov/os/2008/03/P064101tech.pdf>.

³ "...the protection of a person's general right to privacy – his right to be let alone by other people – is like the protection of his property and of his very life, left largely to the law of the individual States." *Katz v. United States*, 389 U.S. 347 (1967).

⁴ Robert Ellis Smith & James Sulanowski, Compilation of state and federal privacy laws (Privacy Journal 2002 ed. 2002).

⁵ Paul Schwartz, Preemption and Privacy, 118 Yale L. J. 902 (2009).

⁶ California Office of Information Security and Privacy Protection, Privacy Laws, Jul. 20, 2009, available at http://www.oispp.ca.gov/consumer_privacy/laws/.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

prescriptive, detailed regulation. For instance, the Fair Credit Reporting Act mandates an evolving “maximum possible accuracy” standard. Second, in the direct marketing context, the US has imposed advertiser liability for violations of telemarketing, fax, and spam laws. This is a promising approach to address the use of difficult-to-identify and prosecute service providers that are responsible for illegal marketing campaigns. Third, audit requirements for access to personal information has had a profound effect in encouraging industry and citizen policing of privacy violations. Audit logs have substantiated long-suspected privacy problems regarding “browsing” of files, and news media access to celebrities’ medical records. Fourth, the US has briefly experimented with “data provenance,” a requirement that buyers of personal information exercise diligence to ensure against misuse of data. Data provenance responsibilities can create incentives to reduce gray and black market sales of personal information. Finally, most federal privacy law acts as a floor of protections, allowing states to enact stronger rules. This has created a tension between state and federal governments, resulting in a levelling up of protections, because states (which tend to be more activist on privacy issues) can act where the US Congress is occupied with other issues.

1. Political and Economic Context

The United States of America is a federal constitutional republic of 50 states. At the federal level, legislative, judicial, and executive branches create, interpret, and execute laws. All three branches have a role in privacy law. The federal legislative branch’s two bodies, the House of Representatives and the Senate, promulgate laws. The judicial branch interprets existing law, and may find privacy rights in the Constitution or through common law development. Increasingly, the executive branch creates privacy law for two reasons. First, Congress now tends to write privacy laws that grant federal agencies authority to protect privacy, and along with the responsibility of writing the rules that will govern the sector. Second, the executive is responsible for public safety and its attendant policy implications, many of which are framed as a pitched battle between security and information privacy rights.

Historically, consumer protection has been a state responsibility, thus, a wide range of state interventions (from family law, to medical law, and the criminal code) contain privacy protections.⁷ Generally speaking, federal privacy law in the US does not “preempt” (supersede) the privacy rights created by the 50 states. Federal statutory and constitutional privacy law acts as a floor that states may enhance with stronger protections. This has resulted in “defensive pre-emption,” situations where industries have rushed to Congress to supersede strong state laws with “ceiling” preemption. Ceiling preemption prevents inferior political bodies from creating stronger protections.⁸

US lawmakers tend to see their role as neutral “referees” between different political factions, rather than philosopher kings attempting to find the “right answer” to public policy questions. Strong, cohesive minority interests are very effective in swaying lawmakers to their position. In the information privacy field, institutions opposed to the creation of information privacy rights are more cohesive and goal oriented than advocates of privacy laws, who have loose

⁷ Robert Ellis Smith & James Sulanowski, *Compilation of state and federal privacy laws* (Privacy Journal 2002 ed. 2002).

⁸ Professor Paul Schwartz discusses next-best alternatives to ceiling preemption, including sunsets that cause preemption to expire, and approaches that allow a single state to enact strong protections to prevent a chaotic landscape of laws. See Paul Schwartz, *Preemption and Privacy*, 118 Yale L. J. 902 (2009).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

roots grounded across the political spectrum, and may see privacy as a second-tier issue in their advocacy.⁹ Consonant with the American tradition, scores of organizations advocate for privacy in the US. The most prominent include the Electronic Privacy Information Center, the Center for Democracy & Technology, the Electronic Frontier Foundation, the Privacy Rights Clearinghouse, and the American Civil Liberties Union.

Omnibus privacy legislation would face a number of challenges in the US Congress for passage. Such privacy legislation would touch upon so many different aspects of commerce that the law would be referred to many different committees. The legislation would have to be marshalled through each committee before passage, and in the process would be altered according to the provincial desires of each committee, or delayed, or simply stopped. This is particularly true in the upper house, the Senate, where a single member can anonymously place a “hold” on legislation to stop its progress. In fact, in 2003, when online privacy legislation started progressing in the Senate, the arcane “two-hour rule” was employed to stop all Senate business the day a popular privacy bill came up for a vote in committee.

A strong, united range of groups is active in limiting the extension of information privacy rights. Political opponents range from moneyed technology firms, to law enforcement, to interest groups that may favour information privacy protections in some contexts but strongly oppose it in others. To amplify the opposition, these groups also fund a set of libertarian-leaning political groups that transmit free market rhetoric in debates concerning consumer protection. Public relations firms are employed as well.

In recent years, the financial services industry has solidified as a formidable opponent to information privacy rights. In 1999, financial services firms (banks, brokerages, and insurance companies) strongly opposed but ultimately failed to block a privacy law for customer records. (That law, the Gramm-Leach-Bliley Act, will be discussed further in other sections of this report.) This law requires notice of privacy practices, a right to opt out of information sharing with third parties, and security safeguards for customer records. The financial services industry favoured a “no opt” system. Implementation of the law was extremely costly, and requires institutions to vet all of their service providers to ensure that they have safeguards for customer information. As a result, financial services institutions have lined up to support other industries that face new privacy laws, to prevent obligations from becoming more stringent than Gramm-Leach-Bliley. Most notably, the financial services industry has walked in lockstep with commercial data brokers in opposition of new privacy laws. Apparently the financial services industry opposes new privacy laws, but if enacted, they wish to ensure that rights and responsibilities are compatible with and no broader than their current obligations under Gramm-Leach-Bliley.

2. Surveillance context

The law of government surveillance is controlled by the US Constitution, sectoral statutes, and administrative regulations. As with consumer privacy approaches, sectoral statutes in the surveillance context has created an uneven landscape of protections for personal information.¹⁰ Some of the strongest protections for information held by private actors apply

⁹ Colin J. Bennett, *The privacy advocates : resisting the spread of surveillance* (MIT Press 2008).

¹⁰ For an excellent illustration of this landscape, see Center for Democracy & Technology, *Government Access to Papers, Records, and Communications*, 2006: <http://www.cdt.org/wiretap/govaccess/govaccesschart.html>.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

to Video Rental companies; while many other businesses can volunteer customer information to law enforcement.

Wiretapping for criminal prosecution and anti-terrorism purposes is regulated by federal and state laws. Generally speaking, these laws do not limit visual surveillance, but instead focus on monitoring of electronic communications. Federal law follows a one-party consent model, meaning that government agents can record conversations so long as it obtains the consent of one party to the conversation.¹¹ Twelve states require all-party consent for recording conversations.¹²

The terrorist attacks of September 11, 2001 have radically altered the surveillance context in the US. Shortly after the attacks, Congress enacted the USA PATRIOT Act, which expanded government wiretapping powers.¹³ In addition to the PATRIOT Act, Congress also enhanced law enforcement ability to gain access to personal information through the passage of the Cyber Security Enhancement Act.

In December 2005, it was reported in the New York Times that former President Bush ordered the National Security Agency to conduct widespread domestic surveillance.¹⁴ The full extent of this surveillance is unknown, but investigative reporting suggests a network of “fire hose” style data monitoring of central hubs of communications data.

While the US has not mandated a national identity card, federal law requires states to develop standardized drivers licenses that may be required for individuals to board planes or to enter federal buildings. Practically speaking, a combination of tax identification numbers (the Social Security number) and state-issued drivers licenses form the nation’s identity system. Many Americans do not have a passport. Both the federal and state governments are heavily dependent upon private-sector companies (commonly called “commercial data brokers”) to obtain basic, up-to-date contact information on citizens.

3. Social attitudes to privacy

Americans frame a wide array of individual interests as “privacy rights.”¹⁵ Notions of privacy include physical isolation, “decisional” privacy (right to contraception, access to abortion, procreation, marriage, and child rearing preferences), and of course, information privacy.¹⁶ This wide range of interests, combined with the US sectoral approach, causes privacy rights to be rooted in constitutional law, statutory law, common law, agency regulations, self-regulatory principles, and social norms. Within each of these categories, privacy rights are found in no single, coherent expression.

¹¹ 18 USC § 2511(2)(d).

¹² Reporters Committee for Freedom of the Press, Can We Tape? (2008) available at <http://www.rcfp.org/taping/index.html>.

¹³ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, P.L. 107-56 (2001).

¹⁴ James Risen & Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. Times, Dec. 16, 2005.

¹⁵ Daniel J. Solove, Conceptualizing Privacy, 90 California Law Review 1087 (2002), <http://www.jstor.org/stable/3481326>.

¹⁶ Daniel J. Solove, A Taxonomy of Privacy, 154 U. Penn. L. Rev 477 (2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

This lack of coherence may flow from Americans' attitudes towards privacy rights. In 1995, Professor Priscilla Regan concluded that: "Both historical examples and the results of public opinion surveys demonstrate that people value privacy as an ideal that is important in the abstract and as a factor that is understood in real-life situations...a great deal of latent public policy concern about privacy exists."¹⁷ Professors Samuel J. Best, Brian S. Krueger, and Jeffrey Ladewig, in their review of 15 years of privacy polls, concluded that, "Americans have maintained that privacy is an important right in the abstract."¹⁸

Professor Alan Westin has pioneered a popular "segmentation" of privacy attitudes among the American public to gauge their concern.¹⁹ In it, Americans are divided into three groups: "Privacy Fundamentalists," who place a high value on privacy and favor passage of strong privacy laws; "Privacy Pragmatists," who see the relative benefits of information collection and favor voluntary standards for privacy protection; and the "Privacy Unconcerned," those who have low privacy concern and have little objection to giving government or businesses personal information. Westin has argued that public policy should serve the privacy pragmatists, as it is a group understood to represent a reasonable middle ground.²⁰

However, when Americans' knowledge of privacy rights is explored, one finds that most consumers falsely believe that privacy protections exist where they do not. For instance, Turow et al.²¹ found in a national study that Americans falsely believe that privacy policies prohibit the sale of personal information.²² Further research performed by Hoofnagle and King (focusing only on Californians) shows that the knowledge gap is substantial; that Californians falsely believe that privacy policies guarantee a set of vigorous privacy rights. Importantly, those identified as privacy pragmatists and privacy unconcerned are the most likely to misunderstand business practices, technological capability, and the law.²³ Thus, a false belief that privacy laws already regulate many practices may explain why so many Americans say that existing laws adequately protect individuals' rights.

The US system is anathema to some. It is riddled with loopholes. It under-protects genuinely harmed individuals, while in other cases, rewards individuals who have suffered minor

¹⁷ Priscilla M. Regan, *Legislating privacy: technology, social values, and public policy* (University of North Carolina Press, 1995).

¹⁸ Samuel J. Best, et al., *Privacy in the Information Age*, 70 *Public Opin Q* (2006), available at <http://poq.oxfordjournals.org/cgi/content/abstract/70/3/375>.

¹⁹ Ponnurangam Kumaraguru & Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin's Studies*, Tech. rep. CMU-ISRI-5-138 Institute for Software Research International (ISRI), Carnegie Mellon University (2005), available at <http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf>.

²⁰ Westin, Alan K. 2001. *Opinion Surveys: What Consumers Have To Say About Information Privacy*, before the House Commerce Subcommittee on Commerce, Trade, and Consumer Protection, May 8, 2001 (testimony of Alan K. Westin, Professor Emeritus, Columbia University), available at: <http://energycommerce.house.gov/reparchives/107/hearings/05082001Hearing209/Westin309.htm>.

²¹ Turow, Joseph, *Americans & Online Privacy, The System is Broken*, Annenberg Public Policy Center, June 2003, available at:

http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf; Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun. 1, 2005.

²² Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 *ISJLP* 723 (2007), available at <http://www.is-journal.org/>.

²³ Chris Jay Hoofnagle & Jennifer King, *Research Report: What Californians Understand About Privacy Offline* (2008) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

privacy invasions. It treats individuals in public places, and in particular, public figures, as fair game to gross treatment.

Nevertheless, it must be said that information-dependent, critical businesses were hatched and thrived in this environment. Some of these businesses are now critical to the maintenance of a consumer economy; others are simply fun, and as much as they contravene basic privacy principles of collection and use limitations, consumers love them.

Perhaps Americans' acceptance of the sectoral approach is naïve and without truly informed consent. To explore this idea, consider the recent example of Facebook.com's "Beacon" service. It serves as an excellent example of American consumers' information privacy norms and the gulf between consumers' knowledge and actual business practices. The structure of Facebook.com allows its users to quickly organize and express discomfort with the company's policies. Three recent policy changes sparked Facebook revolts: news feed, the "Beacon" program, and a terms of service policy change. The news feed feature allowed Facebook users' friends to track their use of the site. Beacon was similar, in that it allowed users' friends to view their purchases on partner websites. The terms of use apparently gave Facebook a perpetual license to use user-submitted content, even after accounts were terminated. These three policy changes are not uncommon in American e-commerce. Sites routinely sell information about user activity and purchase behaviour. And many sites reserve a broad range of rights to user-submitted data, even after an account is cancelled. When given adequate attention and a mechanism to object, users expressed great concern about these three practices.

The Facebook example suggests that, armed with salient experiences, transparency, and a medium to express regret, Americans would object to many common business uses of personal information.

4. International obligations in relation to privacy

The U.S. Department of Commerce has developed a "safe harbor" system in order to insulate self-certifying companies from prosecutions by European authorities under European privacy laws.

The US is a founding member of the Organization for Economic Cooperation and Development (OECD). The US achieved observer status at the Council of Europe in 1995. The US is a member of the Asia-Pacific Economic Community (APEC). In 2006, the US ratified the Council of Europe Convention on Cybercrime.

5. Constitutional protections

Constitutional

While privacy is not explicitly mentioned in the US Constitution, a series of cases have created a substantive due process right to information privacy. In *Griswold v. Connecticut*, the Supreme Court recognized a "zone of privacy" created by the "penumbras" of the First, Third, Fourth, Fifth, and Ninth Amendments.²⁴ A right to privacy can be inferred through

²⁴ 381 U.S. 479 (1965).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

these amendments; the first cases construing the contours of this right found support for limiting state inference in contraception and marriage.

The Constitutional right to information privacy was set in motion by *Whalen v. Roe*,²⁵ but was never pursued again by the Supreme Court. Nevertheless, many of the courts of appeal (inferior courts just below the Supreme Court) have recognized a right to information privacy in the US Constitution.

A well-known test for the constitutional right to information privacy is found in *US v. Westinghouse*, where the Third Circuit Court of Appeals articulated a seven-part test:²⁶ a court will consider the type of record requested, the information the record contains, the potential for harm in any subsequent non-consensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to protect the information, the degree of need for access to the information, and whether there exists an express statutory mandate or other public policy militating toward access.

The First Amendment to the US Constitution contains the country's guarantees for free expression. The First Amendment protects individuals' rights to associate²⁷ and to speak anonymously.²⁸ In recent decades, advertising has received increased protection under the First Amendment as "commercial speech."²⁹ Commercial speech is expression that relates solely to the economic interests of the speaker. Government can regulate truthful commercial speech where a substantial government interest is advanced by the regulation, and where there is a reasonable fit between the government interest and the regulation. False or misleading commercial speech is not protected by the First Amendment.

As protections for commercial speech grew, it formed the basis for challenges to information privacy laws. In 1999, a US federal circuit court held in *U.S. West* that opt-in consent restrictions on secondary uses of telephone records violated commercial free speech rights.³⁰ However, since that decision, courts have consistently upheld data-protection-style privacy laws against First Amendment challenges, and a recent case suggests that courts may not view information sale as "speech" at all. The Fair Credit Reporting Act,³¹ the financial privacy laws,³² and the telemarketing laws³³ have all withstood First Amendment attacks. Despite the 1999 *U.S. West* decision, a different Circuit Court recently held that FCC opt-in regulations are constitutional.³⁴ And most notably, the First Circuit Court of Appeals recently held in *IMS Health* that a law prohibiting use of prescriber-identified prescription

²⁵ 429 U.S. 589 (1977).

²⁶ 638 F.2d 570 (3rd Cir. 1980).

²⁷ *NAACP v. Alabama*, 357 U.S. 449 (1958).

²⁸ *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995).

²⁹ *Central Hudson v. PUC*, 447 U.S. 557 (1980).

³⁰ *US West v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000).

³¹ *Trans Union v. FTC*, 245 F.3d 809 (D.C. Cir. 2001), *rehearing denied*, 267 F.3d 1138 (2001), *cert. denied*, 122 S. Ct. 2386 (U.S. 2002).

³² *Trans Union v. FTC*, 295 F.3d 42 (D.C. Cir. 2002), *rehearing en banc denied*, *Trans Union v. FTC*, 2002 U.S. App. LEXIS 22105 (D.C. Cir. Oct. 22, 2002).

³³ *Destination Ventures, Ltd. v. F.C.C.*, 46 F.3d 54 (9th Cir. 1995); *Moser v. FCC*, 46 F.3d 970 (9th Cir. 1995) *cert. denied*, 515 U.S. 1161 (1995); *Minnesota v. Sunbelt Communications and Marketing*, 2002 WL 31017503 (D. Minn. Sept. 4, 2002); *Texas v. American Blastfax, Inc.*, 121 F. Supp. 2d 1085 (W.D. Tex. 2000); *Kenro, Inc. v. Fax Daily, Inc.*, 962 F. Supp. 1162, 1167 (S.D. Ind. 1997); *Missouri ex rel. Nixon v. American Blast Fax, Inc.*, Missouri ex rel. Nixon v. American Blast Fax, Inc. 323 F.3d 649 (C.A.8 2003).

³⁴ *National Cable & Telecommunications Ass'n v. F.C.C.*, 555 F.3d 996 (C.A.D.C. 2009).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

records (doctors' prescription writing histories) was a regulation of conduct, not speech, and even if a regulation of speech, it would survive commercial speech analysis.³⁵ The Supreme Court denied review of the case.³⁶

While data-protection-style privacy laws have survived commercial speech challenges, the privacy torts have been greatly pruned by US First Amendment jurisprudence. See discussion below, at 6.

The Constitutional basis for privacy law on the federal level is not discussed further here, as its application to private actors is extremely limited. At least at the federal level, the Constitution operates mainly to restrain government access and use of information.

California Constitutional Protections for Privacy

The California Constitution explicitly recognizes a right to privacy. Proposition 11 added privacy to the list of enumerated inalienable rights enjoyed by Californians. Passed in a general election in 1972, 62.9% (4,861,225) of voters supported it, 37.1% (2,871,342) opposed the measure.³⁷ Article 1 § 1 reads: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

In *Hill v. National Collegiate Athletic Assn*, the California Supreme Court held that the State's privacy provision applied to private-sector actors.³⁸ This extension of the Constitution to private actors only protects individuals against serious invasions of privacy.³⁹ In order to state a successful claim, a plaintiff must establish a legally protected privacy interest (including dissemination or misuse of personal information), a reasonable expectation of privacy under the circumstances, and a serious invasion of a privacy interest.⁴⁰

Even if a claim is established, the defendant can affirmatively assert that that the invasion of privacy is justified because it substantively furthers one or more countervailing interests.⁴¹ Thus, in *Hill*, the Supreme Court held that urinalysis of college athletes implicated privacy

³⁵ *IMS Health Inc. v. Ayotte*, 550 F.3d 42 (1st Cir. 2008).

³⁶ *IMS Health, Inc. v. Ayotte*, --- S.Ct. ---, 2009 WL 811508, 77 USLW 3562, 77 USLW 3706, 77 USLW 3708 (U.S. Jun 29, 2009) (NO. 08-1202).

³⁷ The supporters of Proposition 11, Assemblyman Kenneth Cory and Senator George R. Moscone made a broad appeal to curb government and business incursions into information privacy: The pair wrote of "government snooping," the building of "cradle-to-grave" profiles, the problem of secret government databases, data inaccuracy, the inability to correct databases, and personal information in public records: "The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information...."

³⁸ 865 P.2d 633 (Cal. 1994).

³⁹ *Pioneer Electronics (USA), Inc. v. Superior Court*, 150 P.3d 198 (Cal. 2007) (disclosure of identities of consumers who complained of product to plaintiff in class action suit was not a serious invasion of privacy).

⁴⁰ *International Federation of Professional and Technical Engineers, Local 21, AFL-CIO v. Superior Court*, 165 P.3d 488 (Cal. 2007).

⁴¹ 865 P.2d 633, 656 (Cal. 1994).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

interests, but the countervailing interests in ensuring fair competition and preventing drug use outweighed the athletes' privacy interests.

New Jersey Constitutional Protections for Privacy

New Jersey is one of eleven states that have interpreted state constitutions to provide a much broader scope of protections than the US Constitution. Under the US Constitution, the Fourth Amendment protects individuals who have a reasonable expectation of privacy. The Supreme Court has interpreted this rule to not provide privacy protection when individuals share information with third parties. Thus, when law enforcement seeks bank records, telephone calling records, ISP registration records, or even email header and IP address information, it does not implicate the Fourth Amendment, because individuals have entrusted this information to a third party.⁴²

New Jersey has interpreted its constitution to provide protections in these contexts, albeit in a limited fashion, and only with regard to government acquisition of information. Recently, in *State v. Reid*, the New Jersey Supreme Court held that individuals have a reasonable expectation of privacy in ISP records. The State could still acquire these records using a properly executed grand jury subpoena. New Jersey's constitution has been interpreted to protect phone records, garbage left for collection, electric usage records, and bank records.⁴³

⁴² Stephen Henderson, Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search, 55 *Catholic University Law Review* (2005), available at http://works.bepress.com/cgi/viewcontent.cgi?article=1002&context=stephen_henderson.

⁴³ See e.g. *State v. Domicz*, 873 A.2d 630 (N.J.Super.A.D.,2005): "Since the Supreme Court's 1975 departure from *Schneckloth*, the scope of Article I, paragraph 7 has been found to expand beyond the parameters of the Fourth Amendment in many instances. Our courts have, for example, determined that the state constitution provides an accused automatic standing to complain of an unlawful search and seizure, compare *State v. Alston*, 88 N.J. 211, 440 A.2d 1311 (1981) (retaining the former federal automatic standing rule) with *Rakas v. Illinois*, 439 U.S. 128, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978) (only those with a reasonable expectation of privacy have Fourth Amendment standing); recognizes a reasonable expectation of privacy in the telephone numbers called by an accused from his telephone, compare *State v. Hunt*, supra, 91 N.J. 338, 450 A.2d 952, and *State v. Mollica*, 114 N.J. 329, 554 A.2d 1315 (1989) (holding that the requirements of *Hunt* also apply to a hotel room telephone used by the accused), with *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); recognizes a reasonable expectation of privacy in the records maintained by a financial institution regarding an accused's bank account, compare *State v. McAllister*, 366 N.J.Super. 251, 264, 840 A.2d 967 (App.Div.), certif. granted, 180 N.J. 151, 849 A.2d 183 (2004) with *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976); recognizes a reasonable expectation of privacy in garbage in opaque containers left at the curb for collection, compare *State v. Hempele*, 120 N.J. 182, 576 A.2d 793 (1990) with *California v. Greenwood*, 486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988); rejects the inclusion of a "good faith" exception to the exclusionary rule, compare *State v. Novembrino*, 105 N.J. 95, 519 A.2d 820 (1987) with *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984); recognizes a broader concept of seizure than does the Fourth Amendment, compare *State v. Tucker*, 136 N.J. 158, 642 A.2d 401 (1994) with *California v. Hodari D.*, 499 U.S. 621, 111 S.Ct. 1547, 113 L.Ed.2d 690 (1991); recognizes that a warrantless arrest for a motor vehicle offense does not authorize the search of a vehicle's passenger compartment, compare *State v. Pierce*, 136 N.J. 184, 642 A.2d 947 (1994) with *New York v. Belton*, 453 U.S. 454, 101 S.Ct. 2860, 69 L.Ed.2d 768 (1981); recognizes that there must be a reasonable and articulable suspicion of criminal wrongdoing as a prerequisite to requesting consent to search after a routine stop for a motor vehicle violation, compare *State v. Carty*, 170 N.J. 632, 790 A.2d 903 (2002) with *Schneckloth*, supra (imposing no such requirement for Fourth Amendment purposes); and recognizes that the State must prove by clear and convincing evidence, and not a mere preponderance of the evidence, that the police would have obtained a search warrant independent of the tainted knowledge or evidence previously obtained, compare *State v. Holland*, 176 N.J. 344, 823 A.2d 38 (2003); *State v. Sugar*, 100 N.J. 214, 495 A.2d 90 (1985) with *Murray v. United States*, 487 U.S. 533, 108 S.Ct. 2529, 101 L.Ed.2d 472 (1988); *Nix v. Williams*, 467 U.S. 431, 104 S.Ct. 2501, 81 L.Ed.2d 377 (1984)."

6. Common Law

The common law has evolved causes of action to address privacy wrongs, but the ability of these approaches to address new challenges is limited. The common law torts are notable for their variety—their different expressions protect individuals from false information, from revelation of true information, and from commercial uses of identity.⁴⁴

Four causes of action are widely recognized in state courts; they are known as the “privacy torts.”⁴⁵ They are: intrusion upon seclusion, publicity given to private facts, false light, and appropriation. Generally speaking, the privacy torts have not been successful in stemming privacy violations, either online or offline, because of three major factors: first, to prevail, plaintiffs must establish some type of harm. Absent economic damages, courts are unlikely to provide protection in tort law. Second, the First Amendment operates to severely restrict the torts of publicity given to private facts and false light. In the online context, these torts simply do not map to many of the problems posed by new technologies, with an exception of the public disclosure tort. Third, and most obviously, the privacy torts evolved in the context of interpersonal interactions and media intrusions upon individuals’ lives. Thus, they never evolved responses to modern privacy dilemmas, such as information collection by third parties that lack duties or interaction with individuals.

According to the Restatement on of the Law on Torts (Second), an intrusion upon seclusion occurs where: one intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, if the intrusion would be highly offensive to a reasonable person. Intrusions need not be a physical invasion, but most intrusions involve some investigation into a private space. For instance, a landlord was liable for intrusion for planting a listening device in a tenant’s bedroom⁴⁶

Intrusions can be found in public places. Consumer advocate Ralph Nader, for instance, was intruded upon by investigators who followed him so zealously that they were able to collect confidential information about him.⁴⁷ Obviously, the requirement for an intrusion into private affairs makes this tort irrelevant to many of the commercial privacy problems online. According to the Restatement of the Law on Torts (Second), Publicity Given to Private Life occurs where “one...gives publicity to a matter concerning the private life of another” if the matter is of a kind that would be highly offensive to a reasonable person, and is not of legitimate concern to the public. Thus, publicity given to private facts that are newsworthy is not actionable. Furthermore, the First Amendment’s application to this tort limits it severely. If the private fact relates to a matter of public concern, the government cannot punish publicity given to it unless the government has a compelling state interest. Facts that appear in a public record, even if non-newsworthy and relating only to matters of private concern, will not support a publicity action. The First Amendment immunizes information in the public record from private fact actions.

Despite the limits on the publicity given to private life tort, this right of action may offer a remedy to those who have personal data exposed online. A victim/plaintiff would have to

⁴⁴ For an in-depth discussion of the privacy torts, their scope, context, and limitations, see Daniel J. Solove, A Taxonomy of Privacy, 154 U. Penn. L. Rev 477 (2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622.

⁴⁵ Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998).

⁴⁶ Hamberger v. Eastman, 106 N.H. 107 (1964).

⁴⁷ Nader v. General Motors Corp, 255 N.E.2d 765 (Ct. App. NY 1970).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

prove harm and go through the process of bringing suit (which may in itself publicize the matter further).

According to the Restatement of the Law on Torts (Second), false light occurs where one gives publicity to a matter concerning another that places the other before the public in a false light. This false light must be highly offensive to a reasonable person, and the actor must have knowledge of or acted in reckless disregard as to the falsity of the publicized matter. Like defamation, the First Amendment strongly limits the applicability of the false light tort. If the matter pertains to a public figure or to a matter of public concern, the individual must prove that the speaker acted with actual malice.

According to the Restatement of the Law on Torts (Second), Appropriation of Name or Likeness occurs where one appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy. This last tort has been interpreted very broadly, and lacks significant First Amendment and newsworthiness limitations that apply to the other torts. If the average consumer is placed in an advertisement, recovery is possible.

The academic literature considers several different ways in which tort law could be changed to accommodate data privacy rights.⁴⁸ Yet, individuals have not been successful in employing it to limit commercial use of personal data.⁴⁹

II. Legislation

In the first three sections in this part, we will briefly examine Federal and State statutes (the latter by reference to the example of California), and the case-by-case development of privacy rules by the Federal Trade Commission (FTC). We will then try to see whether, and if so that what extent, the various elements of European data protection law can perhaps be said to be reflected in the laws in the USA.

1. Federal statutes

In statutory law, privacy rights are found in the criminal code, the civil code, evidentiary law, family law, property law, contracts, and in administrative regulations. No single overarching statute even attempts to unify these interests in the diverse contexts in which “privacy” is used to frame some value.

Even so, Congress has created a wide array of statutes to govern the collection, use, and dissemination of personal information. They include:

- (1) Fair Credit Reporting Act of 1970 (FCRA)**
(Pub. L. No. 90-32, 15 U.S.C. §§1681 et seq.)

The first federal information privacy law in the United States is highly complex, and includes elements of all eight OECD Privacy Guidelines. The FCRA is a fascinating statute that

⁴⁸ See e.g., Sarah Ludington, Reining in the Data Traders: A Tort for the Misuse of Personal Information, 2006 Maryland Law Review 140, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1008343; Andrew J. McClurg, A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 NW. U. L. REV. 63 (2003).

⁴⁹ Ram Avrahami sued U.S. News & World Reports for selling his name, but the court rejected his action. Ram Avrahami v. U.S. News & World Report, Inc., 1996 WL 1065557 (Va. Cir. Ct.)

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

strikes a bargain for information processing: highly-sensitive personal information can be collected and aggregated for credit, employment, and tenant screening purposes. To facilitate this, Congress eliminated individuals' defamation, invasion of privacy, and negligence suits for such data collection and use, absent malicious intent. This incredible power is balanced by a strong "maximum possible accuracy" standard integral to the statute, that should prevent the collection of irrelevant, unverifiable information, and creates an evolving standard for accuracy in covered databases. As with other federal privacy laws in the US, the FCRA is sectoral; it governs statutorily-defined "consumer reporting agencies," and limits "consumer reports" created by these agencies to certain employment, tenant screening, and credit uses. Consumers now have a right to obtain a free copy of their consumer report, to dispute inaccurate information, to prevent consumer reports for being used for secondary purposes, and to have derogatory information eventually be removed from the report. Unlike many other nations, the US has a positive credit reporting system, meaning that information about responsible payment is included in reports as is derogatory details of accounts past due.

(2) Privacy Act of 1974
(Pub. L. No. 93-579, 5 U.S.C. §552a)

The Privacy Act governs how federal government agencies collect, use, and disseminate personal information of citizens. Like the FCRA, the Privacy Act reflects a broad range of Privacy Guidelines. However, much of its impact has been limited through liberal employment of a "routine use" exception, which has allowed agencies to transfer personal information without violating the statute. A routine use is one that, "is compatible with the purpose for which it was collected." This exemption has been so liberally applied that agencies have created "blanket routine uses" that apply to every information system housed at the agency. For instance, the Department of Defence has created a list of 16 such uses.⁵⁰ Thus, any system of records, no matter its content or context, can be disclosed for law enforcement, counterterrorism, historical archives, and for the "Information Sharing Environment." Specific systems of records may contain their own routine uses, meaning that discretionary information sharing can be quite broad and determined by the agency itself, rather than by Congress.

(3) Family Educational Rights and Privacy Act of 1974 (FERPA)
(Pub. L. No. 93-380, 20 U.S.C. §§1221 note, 1232g)

The FERPA governs how federally-funded educational institutions handle student records. Student records, which include grades, generally cannot be disclosed, even to parents. However, drug and alcohol violations may be reported to parents, if the student is under 21 (the legal drinking age). Importantly, it contains an exemption allowing broad dissemination of "directory" information (which includes basic contact information, student club participation, and photograph), unless a student opts out. An even broader array of information can be disclosed concerning student athletes.

(4) Cable Communications Policy Act of 1984 (CCPA)
(Pub. L. No. 98-549, 47 U.S.C. §551)

Regulates the collection, use, and dissemination of information by cable service providers. In some respects, the CCPA is the strongest US information privacy law. For instance, the law restrains even first party (the cable service provider's) collection of information about

⁵⁰ Department of Defense, Blanket Routine Uses, available at: http://www.defenselink.mil/privacy/blanket_uses.shtml.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

individuals television viewing habits. The CCPA also requires that user data be destroyed after it is no longer needed for service delivery. Still, like the VPPA (discussed below), cable service providers may sell their customer lists to third party marketers on an opt-out consent standard.

(5) Video Privacy Protection Act of 1988 (VPPA)
(Pub. L. No. 100-618, 18 U.S.C. §§2710–2711)

Regulates the collection, use, and dissemination of information by videotape rental companies. Like the CCPA, the VPPA has very strong protections for personal information, and even includes a statutory remedy to prevent introduction of wrongfully-obtained information in court. The VPPA requires opt-in consent before videotape rental companies can sell lists of customers containing the titles of the material they rented. However, the VPPA does allow the sale of mailing lists that include genre information on an opt-out basis. Thus, a videotape rental company cannot sell a list of Jane’s specific rental history without opt-in consent, but it could sell Jane’s contact information and a list of genres that she rents.

(6) Telephone Consumer Protection Act of 1991
(Pub. L. No. 102-243, 47 U.S.C. §227)

Establishes protections for telephone billing records and rights against commercial solicitations. Telemarketing to any phone where the user pays for access fees (such as wireless phones) is governed by a strict opt-in standard, while similar calls to wireline phones are governed by opt out. As originally enacted, telemarketing to wireline phones was governed by a company-specific opt out standard, meaning that consumers had to respond individually to each company engaging in a solicitation. The combined effect of tens of thousands of commercial solicitors caused the President Bush Administration to create a “Do-Not-Call” registry in 2008, creating a single point of contact for opting out of all telemarketing. The FTC originally estimated that 50-60 million numbers would be enrolled in the registry, but over 160 million signed up.⁵¹ A study by Harris Interactive has found that the Do-Not-Call registry was effective in reducing sales call volume for most consumers.⁵²

(7) Driver’s Privacy Protection Act of 1994
(Pub. L. No. 103-322, 18 U.S.C. §§2721–2725)

The DPPA restricts states from disclosing or selling personal information in state motor vehicle records. As with other major US privacy laws, the DPPA was enacted as a result of a controversy—attacks upon and the death of an individual who was located through motor vehicle records. As originally enacted, motor vehicle authorities could sell records to commercial entities on an opt out basis, but in 1998, an opt in standard was adopted. Since then, commercial entities have exploited other loopholes to obtain driver data (see below, at **X**).

(8) Telecommunications Act of 1996
(47 USC § 222)

The Telecommunications Act includes protections for “Customer Proprietary Network Information,” (CPNI) a complex term used to encompass calling records, including the

⁵¹ Federal Trade Commission, The Do-Not-Call Improvement Act of 2007: Report To Congress Regarding the Accuracy of the Do Not Call Registry, Nov. 7, 2008, available at <http://www.ftc.gov/opa/2008/11/dncact.shtm>.

⁵² Federal Trade Commission, Compliance with Do Not Call Registry Exceptional, Feb. 13, 2004, available at <http://www.ftc.gov/opa/2004/02/dncstats0204.shtm>.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

numbers called, numbers received, and new types of information collection, such as location of the user. The Federal Communications Commission recently restricted disclosure of CPNI; carriers must now obtain opt-in consent from customers.

(9) Health Insurance Portability and Accountability Act of 1996 (HIPAA)
(Pub. L. No. 104-191 (Privacy Rule promulgated at 45 CFR § 460))

Resulted in promulgation of rules for the security and privacy of health information. Prior to HIPAA, medical privacy was regulated on a state-by-state basis. HIPAA created national standards that do not preempt state law (thus some state medical privacy protections are more stringent). HIPAA allows transfer of medical information for treatment, payment, or health care operations purposes without patient consent. HIPAA's privacy rule creates requirements for privacy and security training, the appointment of an official responsible for privacy, a right to control appearing in a patient directory, and a right to control how medical information is communicated. Importantly, the rules created access rights to one's medical file, and the right to an auditing of disclosures. Now that auditing and access protections are in place, patients have discovered many cases where authorized users of records have abused their access, and have even sold personal information to news media entities.⁵³

(10) Children's Online Privacy Protection Act of 1998
(Pub. L. No. 106-170, 15 U.S.C. §§6501–6506)

Requires parental consent to be obtained before websites knowingly collect personal information about children (under the age of 13) online, and the posting of a privacy policy. The law also requires that parents have access to their child's information and a right to opt-out of future collection and use. COPPA also limits a site's ability to condition playing games, contests, or other child-oriented activities on disclosing more personal information than is reasonably necessary to participate in that activity.

(11) Gramm-Leach Bliley Act of 1999
(Pub. L. No. 106-102, 15 U.S.C. §§6801–6809)

Created statutory security and privacy rights in information held by financial services institutions (banks, insurance companies, and brokerage houses). Consumers are entitled to yearly privacy notices, and are afforded the ability to opt out of information sharing to third parties. This law contains no private right of action, access rights, collection limitation rights, or right to delete information held by financial services companies.

(12) Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) Act of 2003
(Pub. L. No. 108-187)

Established requirements for the sending of unsolicited commercial email, including an ability for individuals to opt out of unwanted messages. This law contains no private right of action for consumers, but internet service providers (which was broadly defined), may sue for receipt of unwanted email.

⁵³ Former UCLA hospital worker admits selling celeb medical records, USA Today, Dec. 1, 2008, available at http://www.usatoday.com/life/people/2008-12-01-UCLA-records_N.htm.

2. Statutory Protections for Privacy at State level – the example of California

California has passed numerous statutes to address data collection, use, and dissemination. Many of these statutes create a fair information practices framework, on a piecemeal basis. Many of these statutes passed in reaction to public objection to a specific marketing practice, thus, the approach is sectoral and some businesses can design their practices to escape the laws' provisions. Some examples include:

- California law requires operators of commercial web sites to post privacy policies and adhere to representations made. The law requires that the notices specify the categories of personal information collected, categories of information sharing partners, and the effective date of the of the policy.⁵⁴ The law does not set baseline standards for collection, use, and dissemination of information online. Thus, third party information sharing would be compliant with the law, so long as it is disclosed properly.
- California law restricts the public posting of personal information about several categories of public officials and others. For instance, it is illegal to knowingly post home address information of public officials.⁵⁵ Similarly, knowing posting of personal information pertaining to individuals involved in reproductive services, whether as patients, employees, or volunteers, is illegal.⁵⁶ California recently passed legislation creating similar protections for scientists involved in animal research.
- California restricts marketing uses of data in several ways.
 - Long before the Federal Communications Commission adopted opt in rules for sharing of telephone subscriber information, the California Public Utilities Code required written consent for transfer of such information.⁵⁷
 - California prohibits supermarkets from requiring consumers to provide a drivers license or Social Security number when enrolling in a supermarket club/loyalty card program. Supermarkets are further prohibited from selling personal information otherwise collected in the program. Importantly, membership warehouse companies such as Costco and Sam's Club are exempt.⁵⁸
 - The State requires notice and consent before collecting information directly from consumers for medical marketing purposes.⁵⁹
 - Upon request, Californians may request that companies disclose the identities of their third party marketing partners, and may opt out of information sharing with these third parties.⁶⁰

⁵⁴ Cal. Bus. & Prof. Code § 22575.

⁵⁵ Cal. Gov. Code § 6254.21.

⁵⁶ Cal. Gov't Code § 6254.21.

⁵⁷ Cal. Pub. Utilities Code § 2891.

⁵⁸ Cal. Civ. Code § 1749.64.

⁵⁹ Cal. Civ. Code § 1798.91.

⁶⁰ Cal. Civ. Code. § 1798.83.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

- California restricts the creation of a cell phone number directory by requiring telephone companies to obtain written consent before including numbers in such a database.⁶¹ The purpose of this law has been frustrated by its definitions—it only applies to telephone carriers. Thus, database companies are free (and have) created directories of wireless phone number for use without consent of the subscribers.⁶²
- California’s Confidentiality of Medical Information Act requires patient authorization (subject to exception) for disclosures of medical information.⁶³ California limits marketing uses of medical information more strongly than federal law.
- California law prohibits sending unsolicited commercial email to State residents, but the law is preempted by the federal CAN-SPAM Act. The federal law supersedes all state anti-spam laws, except to the extent that these state laws prohibit falsity or deception.
- A host of laws give identity theft victims rights in California. Police must investigate complaints of identity theft. Victims can bring suit to obtain a judicial declaration that they are innocent of crimes committed by the thief. Victims can obtain records of fraudulent transactions and account information.
- Californians enjoy stronger financial privacy rights than federal law affords. Third party information sharing is governed by an opt in standard in California (opt out in federal law).⁶⁴ Californians can also opt out of affiliate sharing by banks.
- California requires secure destruction of personal information many contexts. Businesses that collect personal information have a duty to take all reasonable steps to destroy data by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.⁶⁵ A separate provision of the code places destruction duties upon companies with medical data.
- California was the first state to pass “security breach notification” laws, which require entities with sensitive personal information to inform individuals when that data is acquired by an unauthorized individual. These laws have been mirrored in at least 45 states. In addition to notification, many businesses are subject to general information security rules imposed by California’s AB 1950. Businesses must maintain reasonable security procedures appropriate to the nature of the information to prevent unauthorized access, destruction, use, modification, or disclosure.⁶⁶
- California has been an innovator in credit reporting. California was the first state to pass credit “freeze” legislation. This legislation allows a consumer to lock their credit report so that new credit issuers cannot access it, thus preventing new account identity

⁶¹ Cal. Pub. Utilities Code § 2981.1.

⁶² See e.g. Intellius, <http://www.intellius.com/people-search-phone.html>; TargusInfo, <http://www.targusinfo.com/about/data/>.

⁶³ Cal. Civ. Code § 56.

⁶⁴ Cal. Fin. Code § 4050.

⁶⁵ Cal. Civ. Code § 1798.81.

⁶⁶ Cal. Civ. Code § 1798.81.5.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

theft. California passed many victim-focused credit reporting protections that were ultimately incorporated in federal law.

- To prevent identity theft, many specific credit card marketing and approval practices are regulated. For instance, when a credit card issuer receives a change of address request and a request for a replacement card, it must send notice of this fact to the old and new addresses.⁶⁷ Issuers must also verify addresses when a consumer returns a credit application with a change of address request.⁶⁸ Both of these protections were incorporated into federal privacy laws by the US Congress. Skimming credit card numbers is illegal.⁶⁹
- California passed the first anti-paparazzi statute in the United States in 1998. That act prohibits “constructive” invasions of privacy: the use of technology to obtain images and sound that could not be captured without a physical trespass. The law also prohibits assaults on individuals committed with the attempt to capture images or recordings of another.⁷⁰

3. Case-by-case development of privacy standards by the FTC

The importance of the FTC case-by-case approach

As already noted, outside of specific privacy statutes, privacy rights are found in the criminal code, the civil code, evidentiary law, family law, property law, contracts, and in administrative regulations. But most relevant to the new challenges is the “federal common law” being created on a case-by-case basis by the Federal Trade Commission (FTC).

It is important to note that the FTC has adopted a more limited set of fair information practices than international authorities. The agency is concerned with notice, choice, access, security, and accountability. There has been almost complete inattention to the right of access, as the agency sees access as heightening security risks and potentially triggering a requirement to collect more personal data. In recent years, a heavy emphasis has been placed on security.

The FTC’s focus on information security has nuanced implications for privacy rights. In the US privacy is often equated with security.⁷¹ But more specifically, business groups tend to frame privacy laws as security mandates. In rulemaking, this results in an emphasis on securing personal information, while other aspects of fair information practices are subordinated (for instance, the FTC has subordinated access rights to security concerns, because of the risk of records being released to the wrong data subject). This frame also allows information collectors to adopt a “secrecy theory”⁷² approach to privacy. Under it, a company can engage in maximum data collection, because the information is “private” so long as it remains secret and secure within the company’s systems.

⁶⁷ Cal. Civ. Code § 1799.1b(a).

⁶⁸ Cal. Civ. Code § 1747.06.

⁶⁹ Cal. Penal Code § 502.6.

⁷⁰ Cal. Civ. Code § 1708.8.

⁷¹ Colin J. Bennett & Charles D. Rabb, *THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE* (MIT Press 2006).

⁷² Daniel Solove, *Access and Aggregation: Privacy, Public Records, and the Constitution*, 86 *Minnesota Law Review* 1137 (2002), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=283924.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

The FTC investigates practices that it discovers, those that are revealed by news reporting, and through analysis of consumer and advocate complaints. When conducting a standard investigation, the FTC will not reveal identities of companies, documents obtained, or information discovered in the inquiry process.⁷³ Only when an entire industry is being investigated will the agency issue public notice of its activities.

Investigations typically become public after the agency has issued a complaint alleging violations of the Federal Trade Commission Act (FTCA). Once the agency accepts a consent agreement, it places it in the public record for thirty days of comment before making the agreement final.⁷⁴ Once the agreement becomes final, violators are subject to \$11,000 fines for each violation. In pursuing privacy violations, the FTC employs “unfairness” and/or “deception” under the FTCA.

FTCA: Unfairness

The agency’s unfairness power has been narrowed in the past 20 years, and now focuses upon addressing unjustified consumer injury. The agency considers a three-prong test when pondering consumer injury, and all three are difficult to meet as a consumer wronged by a privacy-invasive business. For a consumer injury to be unfair, it must be substantial, the injury must not be outweighed by countervailing benefits to competition or consumers produced by the practice, and it must be an injury that could not have been reasonably avoided.⁷⁵

Substantial injuries to consumers usually involve monetary harm, coercion into the purchase of unwanted goods or services, and health or safety risks. Substantial injury may also occur where a business practice causes a small harm to a large number of people.⁷⁶ So-called “subjective harms,” such as emotional injury, will not normally support a claim of unfairness.⁷⁷ For instance, the FTC “will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers...”⁷⁸

The FTC has indicated that the unfairness theory could be successful in cases where children’s privacy is violated. In a letter from the FTC to U.S. House Committee on Commerce, the agency wrote:

...in the view of Commission staff, the release of children’s personally identifiable information online, without providing parents with adequate notice and an opportunity to control the information, may result in sufficient injury or risk of injury to meet the Section 5 unfairness standard.⁷⁹

⁷³ FEDERAL TRADE COMMISSION, OPERATING MANUAL .3.3.7, available at <http://www.ftc.gov/foia/adminstaffmanuals.htm>.

⁷⁴ FEDERAL TRADE COMMISSION, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION’S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY, Sept 2002, available at <http://www.ftc.gov/ogc/brfovrwv.html> (last visited Aug. 5, 2004).

⁷⁵ Letter from Michael Pertschuk, FTC Chairman, and Paul Rand Dixon, FTC Commissioner, to Wendell H. Ford, Chairman, House Commerce Subcommittee on Commerce, Science, and Transportation (Dec. 17, 1980), at <http://www.ftc.gov/bcp/policystmt/ad-unfair.htm>.

⁷⁶ *Id.* at n.12.

⁷⁷ *Id.* at 2-3, n.16.

⁷⁸ *Id.*

⁷⁹ FTC Responses to Questions Regarding Electronic Commerce to the Honorable Tom Bliley, Chairman, U.S. House Committee on Commerce, at <http://www.ftc.gov/os/1998/9804/bliley.htm> (last visited Dec. 15, 2000).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

The Injury Must Not Be Outweighed By Countervailing Benefits

Injuries must not be outweighed by countervailing benefits to competition or consumers. The FTC notes that that harm to customers must be "injurious in its net effects."⁸⁰ When evaluating business practices, it will consider costs to the business and consumer, burdens on society from increased paperwork and regulation, burdens on the flow of information, and incentives to innovation.

It Must Be Practically Unavoidable

The injury must not have been one that a customer could reasonably avoid.⁸¹ Noting that some sales techniques prevent customer choice, the FTC focuses on "seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."⁸² For instance, unavoidable injury is more likely to be found where businesses withhold critical price or performance information, where the seller engages in coercion, or where the seller targets vulnerable populations.⁸³

FTCA: Deception

In a 1983 letter to the House Commerce Committee, the FTC outlined a three-prong test used to evaluate whether a deceptive practice is actionable: There must be a representation, omission, or practice that is likely to mislead a consumer, the act or practice is considered from the perspective of a reasonable consumer, and the representation must be material.⁸⁴ Express claims and representations are material, as are representations or omissions involving health, safety, cost, or "other areas with which the reasonable consumer would be concerned."⁸⁵

The FTC evaluates representations and omissions based on their likelihood to mislead, rather than whether the consumer is actually misled. A number of factors can show that a representation was misleading, including a juxtaposition of phrases.⁸⁶ Extrinsic evidence, including expert opinion, consumer testimonials, and surveys may be employed in finding that a statement is misleading.⁸⁷

An extremely broad range of commercial activity can be considered deceptive. For instance, misrepresenting the purpose of a sales contact has been found to be a deceptive practice, as has a failure to perform services promised under a warranty or contract.⁸⁸

⁸⁰ *Id.* at 3.

⁸¹ *Id.*

⁸² *Id.*

⁸³ *Id.*

⁸⁴ Letter from James C. Miller, FTC Chairman, to John D. Dingell, Chairman, House Comm. on Energy and Commerce 5-6 (Oct. , 1984), at <http://www.ftc.gov/bcp/policystmt/ad-decept.htm>.

⁸⁵ *Id.* at 5.

⁸⁶ *Id.* at 2-3.

⁸⁷ *Id.* at n. 8.

⁸⁸ *Id.* at 2.

Trends in Unfairness and Deception

Consistent with the FTC's careful history in engaging new areas of commerce, the agency tends to lead with its deception authority, and use its unfairness authority later. Deception is an easier theory to raise, simply because it relies upon statements voluntarily made by the seller. There is general agreement that sellers should abide by their representations

Unfairness is more controversial, because it sets a normative baseline for business activities, in effect, banning practices. In many FTC cases, the agency has plead both deception and unfairness in its complaints. But beginning in 2004, the agency started to rely upon unfairness alone in certain cases. For instance, in Gateway, a company promised not to sell personal information in its privacy policy, but later changed the policy without consumers' affirmative consent. This was seen as an unfair practice because consumers could not avoid the harm of having their information sold. Unfairness has also been used in information security cases. For instance, in the BJ Wholesale case, the FTC found that poor security protections could rise to unfairness.⁸⁹

The FTC may be close to abandoning the notice and choice framework it has followed over the last 10 years. Senior agency officials have questioned the usefulness of the notice and choice approach. Furthermore, a recent enforcement action settled with Sears Holding Corp points to a more interventionist philosophy that rejects some practices even if notice is given. In the Sears case, the FTC found that the company's use of software that collected sensitive personal information related to online and offline consumer activities were not adequately disclosed to consumers.⁹⁰ Sears, in fact, did make a disclosure of the software's functions, but only in a lengthy end user license agreement. This case is important because it represents a growing conflict between the contract-like approaches typically applied in online privacy debates and a growing interest in substantive consumer protection law that restrains the marketplace even in situations where there is "consent" between consumer and company.

4. Definitions and Core Concepts

The US sectoral approach lacks consistent definitions and has different core concepts depending upon the industry regulated. There are no uniform definitions or core concepts. This makes it difficult to properly compare US and European privacy laws, even in specific areas: one should always first carefully check the precise meaning of particular terms in each context (to the extent that these terms are clarified).

5. Scope

The sectoral system has resulted in narrowly-scoped laws, which attempt to regulate businesses in a piecemeal way.

Some US privacy law could be properly categorized as simple regulation of advertising that has profound consequences for individuals' privacy. For instance, the Telephone Consumer Protection Act (TCPA, discussed above), largely regulates the calling practices of telemarketers, requiring them to honour opt-out requests to the Do-Not-Call Registry. Many

⁸⁹ Press Release, FTC, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), www.ftc.gov/opa/2005/06/bjswholesale.htm.

⁹⁰ In re Sears, FTC 0823099 (2009), <http://www.ftc.gov/opa/2009/06/sears.shtm>.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

consumers think the TCPA creates broader, substantive protections against the use of information. When telephone companies sought to create a directory of cell phone numbers (known as “wireless 411”) so that it would be easier for individuals to call each other, many consumers thought it impossible because they were on the Do-Not-Call Registry. However, nothing in the TCPA restrains marketing collection, use, or disclosure of telephone numbers; the law focuses on how companies call those numbers. Thus, carriers or private database companies are free to create wireless 411 directories.

The narrow scope of the US approach results in problems of underinclusiveness and overinclusiveness.

Under-inclusiveness: Exploiting the Gaps with Regulatory Arbitrage

A substantial weakness of the US sectoral approach comes in the form of business practices that evade the substantive requirements of a privacy law, while collecting the very information that the law seeks to protect. This can be accomplished through strained interpretation of the legal provisions of a sectoral privacy law, or through disruptive technology.

A prime example comes from the Drivers Privacy Protection Act. Recall that the DPPA protects drivers’ motor vehicle records; in particular, it requires affirmative consent for marketing uses of such data. Despite this relatively-recent prohibition, businesses still pursue marketing uses of driver data without consent. For instance, in *Kehoe*, marketers exploited the fact that the state of Florida had not implemented the federal ban on marketing uses of driver data.⁹¹ The marketers in that case argued that since Florida was willing to sell the data, they should be absolved of federal liability for purchasing it without consent. Since the *Kehoe* decision, which resulted in a \$50,000,000 settlement, marketers are still intent upon gaining access to driver data. For instance, a company called Imagitas Marketing gains access to driver data by processing registration mailings on behalf of state motor vehicle authorities, thus leveraging a provision in the law that allows service providers to have access to driver data.⁹² Imagitas Marketing includes commercial mailings inside vehicle registration mailings; this practice is the subject of four lawsuits, however, Imagitas Marketing has prevailed in the first of these four cases.⁹³

Gaps in the sectoral system can also be caused by advances in technology. For instance, the Cable Communications Policy Act provides very strong protections concerning cable television viewing data. It applies to cable service providers. Vendors of popular television appliance devices, such as the Tivo Digital Video Recorder, may collect this very same data (including second-by-second viewing behaviour and decision making) without implicating the CCPA. While Tivo has adopted a privacy policy that is stronger than other marketplace actors, it is subject to the limitations of self-regulatory approaches described below.

⁹¹ *Kehoe v. Fidelity Federal Bank & Trust*, 421 F.3d 1209 (11th Cir. 2005), cert denied *Fidelity Federal Bank & Trust v. Kehoe*, 547 U.S. 1051 (2006).

⁹² *In Re Imagitas Inc., Drivers' Privacy Protection Act Litig.*, M.D. Fla., No. 3:07-md-00002-TJC-HTS (2008).

⁹³ *Id.*

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

Over-inclusiveness: The Sectoral Briar Patch

A related problem with the sectoral approach comes from industries that straddle two or more different regulated sectors; this raises new, difficult privacy problems. How should privacy law address, for instance, a credit card charge at a medical clinic, especially one that is tasked to treating a very specific disease? Is such information medical (thus subject to restrictions on marketing use) or financial services information (thus transferable to affiliates and third parties for marketing purposes) or both?

Even within an industry, changes in how technology is used can create different, counterintuitive standards for protection. For instance, the Cable Communications Policy Act protects viewing information of subscribers to cable service providers, but the strong protections of that act have been held not to apply to internet services provided by cable service providers.⁹⁴ Thus, the CCPA, which was passed in part to address concerns that cable television would result in two-way communication, and the possibility of surveillance into activities taking place in the home, may not apply to the ultimate two-way communication service.

Exemptions

As explained above, US privacy law is sectoral, thus there are no universal exemptions to collection, use, and disclosure of personal information. However, some generalizations can be made.

Most US information privacy laws have specific exemptions for law enforcement access to data. These exemptions range from very liberal access provisions to those that require court oversight and a substantive showing of need. For instance, the Drivers Privacy Protection Act explicitly allows drivers records to be used by any government agency, including courts and law enforcement, without a requirement for a subpoena or court order.⁹⁵ Other privacy laws, such as the Fair Credit Reporting Act, require a court order, or a subpoena of a grand jury, before consumer credit reports are released to law enforcement.⁹⁶ However, basic identification information can be released without court process.⁹⁷ The Cable Communications Policy Act requires law enforcement to obtain a court order (subpoena) and give the subscriber notice.⁹⁸ The Video Privacy Protection Act goes further: law enforcement must give notice to the subscriber and show “probable cause to believe that the records...are relevant to a legitimate law enforcement inquiry.”⁹⁹ That law also includes a suppression remedy barring the use of video rental records from being used as evidence in proceedings if the act is violated.¹⁰⁰

Several US information privacy laws contain national security or counterintelligence exemptions. The Fair Credit Reporting Act includes a counterintelligence exemption for the Federal Bureau of Investigation, allowing that agency to obtain account information on

⁹⁴ *Klimas v. Comcast Cable Communications, Inc.*, 465 F.3d 271, 273 (6th Cir. 2006).

⁹⁵ 18 USC § 2721 (b)(1).

⁹⁶ 15 USC § 1681b(a)(1).

⁹⁷ 15 USC § 1681f.

⁹⁸ 47 USC § 551 (c)(2)(B).

⁹⁹ 18 USC § 2710(c).

¹⁰⁰ 18 USC § 2710(d).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

consumers by submitting a written request,¹⁰¹ full credit reports can be obtained with a court order.¹⁰² However, these access provisions are probably no longer used as a result of post September 11, 2001 amendments to the Act. A catchall provision allows any government agency to obtain a full consumer report by certifying that it is needed for investigation of international terrorism.¹⁰³ Similarly, educational records can be obtained by written application to a court in domestic and international terrorism investigations.¹⁰⁴

Several US information privacy laws have exemptions that allow disclosure of personal information to service providers. This is often a necessary transfer of data in order to deliver products and services. In a recent trend, companies are now required by regulation to perform due diligence on service providers. For instance, financial service providers have to ensure that service providers implement and can comply with security safeguards for financial information.¹⁰⁵

Some US privacy laws have many exemptions, but these exemptions are particular to the context of the data. For instance, the Drivers Privacy Protection Act contains 12 exemptions to the opt-in requirement for disclosure of driver records. These include disclosures for anti-fraud purposes in insurance underwriting, for administering towing of vehicles, and for the operation of toll booths.¹⁰⁶

Territorial scope

US federal privacy law typically applies to the nation's states and territories. State privacy laws apply to their own borders. A company doing business in a state with less stringent privacy protections has to comply with the stronger obligations of other states, when that company interacts with the citizens of the more privacy-protective state. For instance, the California Supreme Court held in 2006 that a Georgia company calling California consumers had to comply with California's heightened restrictions on recording phone calls.¹⁰⁷

6. Data Protection Principles

General considerations

While the US approach is sectoral, the principal information privacy laws do follow a framework of fair information principles. This is not true with respect to all "privacy" laws in the US. Some US privacy laws may be fairly characterized as marketing regulation laws. Thus, the spam and telemarketing laws do not create extensive rights in the use and disclosure of data; instead they regulate how marketers contact consumers.

'Purpose-limitation principle' (use and disclosure limitations)

US privacy law typically allows businesses to use personal information for different purposes, including for marketing, without the data subject's consent. This is because the

¹⁰¹ 15 USC § 1681u(a).

¹⁰² 15 USC § 1681u(c).

¹⁰³ 15 USC § 1681v(a).

¹⁰⁴ 20 USC § 1232g (j)(1).

¹⁰⁵ 16 C.F.R. Part 314.4(d).

¹⁰⁶ 18 USC § 2721 (b).

¹⁰⁷ *Kearney v. Salomon Smith Barney, Cal.*, S. 124739, 9/27/06.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

sectoral system leaves many businesses unregulated. Thus, in many contexts, businesses need not give notice or even offer an opportunity to opt out. For instance, sweepstakes companies are not regulated by any sectoral law, and collect information for resale; as do publishers of media, who resell their subscription lists. Nextmark, a direct marketing company, hosts a search engine that includes 60,000 mailing lists.¹⁰⁸ Much of this information is collected from companies that fall through the sectoral system's gaps (consumer survey companies, sweepstakes operators, etc), and individuals have no statutory rights in the data held by the companies. Even medical information forms the basis of targeted marketing lists. While health care providers are subject to the Health Insurance Portability and Accountability Act's privacy rules, medical information can be collected free of those restrictions through consumer survey research. For instance, lists such as the "Suffering Seniors Mailing List" can be found on Nextmark.com.¹⁰⁹ This purports to include contact information for over 4 million Americans over the age of 55 who completed a survey indicating their medical problems.

Just a handful of laws create explicit purpose limitations. The Cable Communications Policy Act is one example. That law prohibits cable service providers from collecting personally identifiable information from the cable system, except for the limited purposes of providing service.¹¹⁰

The Privacy Act of 1974 sets forth "conditions of disclosure," which is an attempt to limit the purposes for which federal agency systems of records are used.¹¹¹ However, one condition is the "routine use," defined as "for a purpose which is compatible with the purpose for which it was collected."¹¹² The routine use exemption has been used extensively to justify transfers of information, and it operates as a loophole to the purpose-limitation function of the Privacy Act.

The Drivers Privacy Protection Act allows records to be used for 14 different purposes (including any purpose where the individual has given consent).¹¹³ These purposes include insurance underwriting, toll booth operation, law enforcement uses, identity verification, motor vehicle recalls, and administering towing of cars.

Collection limitations

US privacy law generally does not have limitations on collection of personal information. Collection limitation runs counter to the notion of most enterprises, which attempt to collect as much information as possible in transactions. Thus, US businesses generally do not recognize a principle of proportionality in data collection; transactions are not designed to minimize collection, and in some contexts, they are designed to maximize collection of information.

The Privacy Act of 1974 specifies that federal agency systems of records only contain, "such information about an individual as is relevant and necessary to accomplish a purpose of the

¹⁰⁸ Nextmark, Mailing Lists Search Tool, available at <http://lists.nextmark.com/>.

¹⁰⁹ Available at <http://lists.nextmark.com/market?page=order/online/datacard&id=140992>.

¹¹⁰ 47 USC § 552(b).

¹¹¹ 5 USC § 552a(b).

¹¹² 5 USC § 552a(a)(7).

¹¹³ 18 USC § 2721(b).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

agency...”¹¹⁴ This same section requires agencies to collect information directly from the data subject where the data may result in an adverse determination concerning federal benefit programs. This is the most salient collection limitation feature of US privacy laws.

A handful of different collection limitation rules regulate the private sector. The Cable Communications Policy Act limits cable service providers in their information collection efforts. That law specifies that “a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber...” except with consent of the subscriber, to render service, or to detect unauthorized reception.¹¹⁵

The Children’s Online Privacy Protection Act prohibits a website operator “from conditioning a child’s participation in a game, the offering of a prize, or another activity on the child’s disclosing more personal information than is reasonably necessary to participate in such activity.”¹¹⁶

The Fair Credit Reporting Act’s accuracy provisions function as a form of collection limitation. Prior to the Act’s enactment, consumer reporting agencies included “lifestyle” information in consumer reports. This might include information on sexual orientation, consumption of alcohol, the cleanliness of a person’s home, or cohabitation among unmarried adults. The FCRA’s maximum possible accuracy standard operates as a brake on such data collection, because lifestyle facts are subjective and often unverifiable. They cannot be reported in a framework that requires maximum possible accuracy. Thus, consumer reports no longer contain such data.

Data quality obligations

A vast portion of US information collection and processing is not subject to any data quality obligations. Specifically, commercial data brokers and marketers that fall outside the scope of a sectoral law have no duties for accuracy. In principle, these actors are regulated by competition—companies with inaccurate personal information about potential sales leads, debtors, and the like will be punished by the market.¹¹⁷ Additionally, where data quality obligations exist, the law does not create metrics or goal-oriented standards to meet. (One could envision performance standards that required credit reports or some other type of record to meet objective criteria for accuracy, timeliness, and relevancy, but no such standard exists in law.)

The most salient data quality obligations in the US surround consumer reporting. Every year, millions of Americans request their consumer report, and some request corrections of their file. The Fair Credit Reporting Act requires consumer reporting agencies to, “follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.”¹¹⁸ In cases of inaccuracy, a consumer may file a dispute with a consumer reporting agency, and the consumer reporting agency must conduct a “reasonable” investigation within thirty days of receiving the dispute. This reinvestigation

¹¹⁴ 5 USC § 552a(e)(1).

¹¹⁵ 47 USC § 552(b).

¹¹⁶ 16 CFR 312.7.

¹¹⁷ Although there are peculiarities to information sale that weigh in favor of overinclusiveness in files, thus diluting the power of competition to police accuracy in consumer information databases.

¹¹⁸ 15 USC § 1681e(b).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

process has been criticized by privacy advocates as being *pro forma*; while industry actors have characterized it as reasonable.¹¹⁹ Nevertheless, it creates a type of data quality standard.

Data security obligations

Several US privacy laws create sectoral data security obligations, and even where there are gaps in the sectoral approach, Federal Trade Commission actions indicate that companies with certain types of consumer data must take reasonable measures to secure it. Sectoral laws generally require “reasonable” procedures to address security, and some impose specific mandates (these do not include technical mandates). The most notable innovation in the data security field is the security breach notification mandate, a performance-standard type regulation that has significantly increased investment in and awareness of information security problems. This will be discussed in more detail below.

The Fair Credit Reporting Act requires that consumer reporting agencies maintain reasonable procedures to protect the security of consumer reports, and mandates certain approaches: “prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in section 604 [§ 1681b] of this title.”¹²⁰ This language sets forth a flexible, evolving security rule, but its effect has been limited by how it has been implemented by the Federal Trade Commission and by consumer reporting agencies. The FTC allows users of the consumer reporting system to obtain a “blanket certification” of compliance with the security mandate.¹²¹ Even when evidence of wrongdoing is detected, the FTC’s commentary advises a limp-wristed response.¹²²

The Gramm-Leach-Bliley Act requires financial institutions to establish security safeguards to protect the privacy of consumers’ nonpublic financial information.¹²³ The security safeguards rule requires financial institutions to develop and execute security plans with reasonable administrative, technical, and physical safeguards.¹²⁴ More specifically, the rule requires the designation of an employee to manage the security program, the identification of reasonably foreseeable risks to data security, implementation of safeguards to address those

¹¹⁹ Federal Trade Commission, Board of Governors of the Federal Reserve System, Report to Congress on the Fair Credit Reporting Act Dispute Process Submitted to the Congress pursuant to section 313(b) of the Fair and Accurate Credit Transactions Act of 2003, Aug. 2006, available at:

<http://www.federalreserve.gov/boarddocs/rptcongress/fcradispute/fcradispute200608.htm>

¹²⁰ 15 USC § 1681e(a).

¹²¹ 16 CFR § 607(a)(2)(C).

¹²² “A consumer reporting agency *should* take several other steps when doubt arises concerning whether a user is obtaining reports for a permissible purpose from a computerized system...” 16 CFR § 607(a)(2)(E)[emphasis added]. In defence of the FTC, the agency is statutorily barred from promulgating regulations on the FCRA. 15 U.S.C. § 1681s(a)(4). However, the author has argued elsewhere that weak implementation of the FCRA’s § 1681e standard is a substantial contributor to identity theft, because it too easily accepts users into the consumer reporting system and treats them as trusted insiders. Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, in SECURING PRIVACY IN THE INTERNET AGE (Stanford University Press 2008), <http://ssrn.com/paper=650162>.

¹²³ 15 U.S.C. § 6801.

¹²⁴ 16 C.F.R. § 314.3.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

risks, implementation of systems to monitor those safeguards, oversight of service providers, and an ongoing assessment and tuning of the information security program.

In a significant state innovation, the California legislature created security breach notification requirements in 2003. These notification requirements create no prescriptive security rules; rather they are a form of performance metric. If a Social Security number, drivers license number, or account number, paired with name, is accessed by an unauthorized party, the governmental or business entity responsible for the data must give the data subject notice of a breach. Since passage of the California law, at least 46 states now have security breach notification laws, some of which protect a broader scope of personal information. For instance, medical records breaches now require notice to the patient, and in California, to state authorities that have levied fines against health care organizations.

The phenomenon of security breach laws deserves special attention, and suggests that privacy regulations tethered to a company's reputation could be very effective in ensuring "compliance plus." The reputational impact of a security breach is so severe that it has driven tremendous investment in information security (perhaps overinvestment), and has provided transparency on an easily obscured problem. Some companies have dealt with the risk by reducing the collection of sensitive personal information. This performance-standard based regulation has driven information exchange among security professionals, and promoted their importance within organizations. It has also given chief security officers more leverage to invest in and implement encryption and access controls at enterprises.¹²⁵ However it may have less effect on companies without a business to consumer relationship.¹²⁶

Importantly, the security breach notification mandates has shed light on the woeful state of information security at some organizations. In particular, it has elucidated the problem of "browsing" files, most notably at health care organizations visited by celebrities and politicians.¹²⁷

Separately, California imposes general data security requirements through AB 1950.¹²⁸ That law requires businesses with personal information to, "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

Under the President Bush Administration, the Federal Trade Commission led a major effort to raise awareness of information security among businesses and consumers. As part of the effort, the FTC brought enforcement actions against companies under both its deception and unfairness power. For instance, a company was pursued under the agency's deception power for making false representations about security to customers.¹²⁹ Using the agency's

¹²⁵ Samuelson Law, Technology & Public Policy Clinic, Security Breach Notification Laws: Views from Chief Security Officers, Dec. 2007, available at <http://www.law.berkeley.edu/samuelsclinic/privacy/217>.

¹²⁶ Alessandro Acquisti, Alan Friedman & Raul Telang, *Is There a Cost to Privacy Breaches? An Event Study*, PROCEEDINGS OF THE INTERNATIONAL CONFERENCE OF INFORMATION SYSTEMS (ICIS) (2006).

¹²⁷ Peter P. Swire, Peeping, Berkeley Technology Law Journal (forthcoming 2009), available at http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1418091.

¹²⁸ Cal. Civ. Code § 1798.81.5.

¹²⁹ FTC, Guess Settles FTC Security Charges; Third FTC Case Targets False Claims About Information Security, Jun. 18, 2003, available at <http://www.ftc.gov/opa/2003/06/guess.htm>.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

unfairness power, the FTC established a broader principle that even in absence of specific security representations, a company could be liable for not adequately protecting data.¹³⁰

‘Openness’ concerning practices

US law is sparse in requiring openness of practices. Generally, companies now have to post a privacy policy that describes their information collection and use. California law requires companies to post notices specifying the categories of personal information collected, categories of information sharing partners, and the effective date of the of the policy.¹³¹

California is also unique in enacting a direct marketing sunshine law. Known as the “Shine the Light” law, it allows California consumers to request that businesses disclose how they share information with third parties.¹³² Companies can respond to these requests by simply stating that they do not share data, by offering to opt out the consumer, or by disclosing a list of businesses to which the company sold personal data in the previous year.¹³³

In June 2004, Larry Ponemon of the Ponemon Institute surveyed 32 for-profit organizations in California to determine how they planned to comply with the Shine the Light Law.¹³⁴ 56% reported that third-party information sharing would be limited, 34% reported they would revise their customer consent process, and 13% implemented internal audit checks to ensure compliance. The Ponemon study demonstrates how openness can drive companies to engage in less secondary marketing use of data.

Many common information uses need not be disclosed under US law. For instance, many US companies engage in “enhancement” (sometimes referred to as “appendage” or “layering”), a practice where data is added to a customer database. This practice violates the principle that information should be collected from the data subject. Individuals strongly oppose enhancement,¹³⁵ and falsely believe that it is illegal.¹³⁶ Enhancement also contravenes the individual’s expectation that selective revelation will prevent a company from obtaining certain contact information. But the practice need not be revealed in privacy policies.

Companies tend to state their data practices vaguely, and many use terminology that in other contexts has specific legal meaning. For instance, a company may state that it shares personal information with trusted affiliates or partners to market goods. In other contexts,

¹³⁰ FTC, Decision and Order, BJ’s, FTC File No. 042 3160 (2005), available at <http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf>.

¹³¹ Cal. Bus. & Prof. Code § 22575.

¹³² 2003 Cal. SB 27, codified at Cal. Civ. Code § 1798.83-84, available at http://info.sen.ca.gov/pub/03-04/bill/sen/sb_0001-0050/sb_27_bill_20030925_chaptered.pdf.

¹³³ CHRIS JAY HOOFNAGLE & JENNIFER KING, CONSUMER INFORMATION SHARING: WHERE THE SUN STILL DON’T SHINE, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1137990.

¹³⁴ Larry Ponemon, *Shining the Light on Our Personal Information*, Darwin Mag., Nov. 2004 (on file with author).

¹³⁵ Joseph Turow, Lauren Feldman, & Kimberly Meltzer, Open to Exploitation: American Shoppers Online and Offline, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005, available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31> (90% polled disagreed or disagreed strongly with the statement, “If I trust an online store, I don’t mind if it buys information about me from database companies without asking me.”)

¹³⁶ CJ Hoofnagle & J King, What Californians Understand about Privacy Online, SSRN eLibrary (2008), <http://ssrn.com/paper=1262130> (“...42.4% thought privacy policies prohibited enhancement activities, and 12.3% didn’t know”).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

“affiliate” has a specific meaning—it means a company with common ownership or control. “Partner” too communicates a sense of closeness and responsibility that may not be present in a data sale to an arm-length third party. However, in the regime of privacy policies, some companies use these terms as euphemisms for arms-length data sales to companies with no legal affiliation.

Fears of service and price discrimination drive concern over data collection and use practices. However, neither service discrimination nor price discrimination need be disclosed to consumers.

In some respects, information processing is shielded in legally-created obscurity. For instance, under the Fair Credit Reporting Act, consumers are not entitled to know their credit score when obtaining a free consumer report.¹³⁷ Furthermore, consumers are not entitled to know the formula of scores, only the key factors that influence their generation.

Deletion of data

US law generally does not recognize a right of a consumer to require a commercial entity to delete data. The US is generally free of data retention mandates as well. Telephone toll records must be kept for a period of 18 months,¹³⁸ and certain financial, tax, and accounting information must be retained under sectoral rules for a period of 7 years. Businesses must comply with preservation requests by law enforcement, but most businesses are free to keep or delete information as they see fit.

Several sectoral privacy laws require destruction of data after a period of time. The most robust deletion requirements appear in the Cable Communications Policy Act and the Video Privacy Protection Act. The former requires destruction “if the information is no longer necessary for the purpose for which it was collected...”;¹³⁹ the latter requires deletion “as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected...”¹⁴⁰

In the Fair Credit Reporting Act, most derogatory information about consumers is suppressed after 7 years.¹⁴¹ However, consumer reporting agencies do not actually delete this information, because in certain contexts, stale derogatory information can still be reported. For instance, the 7 year suppression mandate is lifted if the report is being accessed for background check purposes, where the prospective employee will be paid more than \$75,000.¹⁴²

The Fair Credit Reporting Act also requires secure deletion of consumer reports. In a broadly applicable rule promulgated by the Federal Trade Commission, any business that uses consumer reports must dispose of records carefully, in order to prevent identity thieves from digging reports out of dumpsters or from recovering files from discarded electronic media.

¹³⁷ 15 USC § 1681g(a)(1)(B).

¹³⁸ 47 C.F.R. § 42.6.

¹³⁹ 47 USC § 551(e).

¹⁴⁰ 18 USC § 2710(e).

¹⁴¹ 15 USC § 1681c(a).

¹⁴² 15 USC § 1681c(b)(3).

7. Areas of special concern

Processing of Sensitive Data

The sensitivity of data does not confer any specific privacy protection to individuals under the US approach. No specific sectoral law addresses processing of sensitive information. Instead, on a sector by sector basis, sensitive information is identified and subject to specific protections. For instance, in the Drivers Privacy Protection Act, photographs, Social Security numbers, and medical information cannot be used as liberally as other motor vehicle information.

The gaps in the US sectoral approach can create confusing results, especially in the context of sensitive information. Medical information can be processed without privacy protections if it is collected by an entity not subject to the Health Insurance Portability and Accountability Act's Privacy Rule. For instance, if a consumer completes a survey attached to a sweepstakes entry or product registration card, that instrument could collect sensitive health information, but it would not be subject to any specific privacy law.

No federal sectoral law addresses private-sector collection and use of Social Security numbers.¹⁴³ However, several states now place restrictions on the collection of the number, and conditions on its use and disclosure.¹⁴⁴ Most notably, security breach notification laws require disclosure to the consumer if Social Security numbers are accessed by an unauthorized party; this has driven companies to reduce their use and storage of SSNs, and has improved security practices.

Automated decisions ('Sensitive Processing')

In a large sense, information processing is explicitly done to perform automated decisions. In at least two contexts, automated decisions are subject to some human interaction. The Privacy Act of 1974, which applies to federal agencies, requires some due process before an adverse action or a decision to reduce or eliminate federal benefits can be taken based upon a data matching program.¹⁴⁵ Before such an adverse action can be taken, the agency must independently verify the information, or engage in a series of procedures that includes giving the individual notice and an opportunity to be heard.

The Fair Credit Reporting Act also requires some process before making adverse employment decisions based on consumer reports. Before an employer makes an adverse action based in whole or part on a consumer report, the employer must provide the individual a copy of the report and a statement of rights under the FCRA.¹⁴⁶

¹⁴³ Government use of the SSN is governed by "Section 7" of the Privacy Act, which requires "[a]ny Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it."

¹⁴⁴ Many of California's restrictions on collection, use, and disclosure have been codified by other states. For an overview of California protections, see: California Office of Information Security and Privacy Protection, Privacy Laws, available at http://www.oispp.ca.gov/consumer_privacy/laws/.

¹⁴⁵ 5 USC 552a(p).

¹⁴⁶ 15 USC § 1681b(b)(3). Technically, the employer is required to obtain consent from the employee before performing a background check.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

Interconnection of files ('Data matching')

In 1998 amendments to the Privacy Act of 1974, the US Congress established some protections for data matching activities of the federal government (discussed above in section 5.2). These provisions added procedural requirements for agencies computer matching in the contexts of benefits. Agencies must provide matching subjects with opportunities to receive notice and to contest adverse information before denial of the benefit. The amendments also require that agencies engaged in matching activities establish Data Protection Boards for oversight. Importantly, these protections only apply in narrow contexts where the government is making decisions concerning benefits programs.

Commercial entities are free to engage in data matching, and do so regularly (see the discussion of commercial data brokers below).

Direct marketing

Business to consumer direct marketing is generally governed by advertising law, by state and federal unfair and deceptive practices laws, and by specific marketing restrictions (such as telemarketing laws). These laws primarily focus upon preventing deceptive or misleading representations and specific types of contact between a marketer and consumer. As a result, US law tends to overlook data *collection and processing* for direct marketing purposes.

A large “list brokerage” industry quietly collects personal information and sells it to generate leads for companies. This industry is totally unregulated, opaque to consumers, and provides a vector for bad actors to contact the vulnerable.¹⁴⁷ For instance, list broker Walter Karl was investigated by the Attorney General of Iowa in 2005 for allegedly selling lists to scam artists.¹⁴⁸ According to an investigative file, the company advertised lists of “impulsive buyers... primarily mature” and “highly impulsive consumers... sure to respond to all of your low-end offers.”¹⁴⁹

Some specific direct marketing activities have been framed as privacy issues and are regulated by privacy law. Telemarketing, unsolicited commercial email (spam), and unsolicited commercial faxes (junk faxes), are all subject to federal and in some contexts, state regulation. Telemarketing is regulated both by the Telephone Consumer Protection Act and the Telemarketing and Consumer Fraud Abuse Prevention Act.¹⁵⁰ These laws create a Do-Not-Call Telemarketing Registry, and a complex set of rules limiting the manner in which telemarketers operate ranging from approved calling times to the number of dropped calls that telemarketers can make. Spam is regulated lightly by the Controlling the Assault of

¹⁴⁷ Karen Blumenthal, How Banks, Marketers Aid Scams, Wall Street Journal, Jul. 1, 2009 (“Other lists offered names, addresses and other data on “Wealthy Widows who Donate” and “Suffering Seniors” who have maladies such as Alzheimer’s and are described as “perfect prospects” for holistic remedies, financial services, subscriptions and insurance.”).

¹⁴⁸ Attorney General of Iowa, A.G. asks Court to Order List Broker to Respond to Telemarketing Fraud Probe State asks court to order list-broker “Walter Karl, Inc.” to cooperate with consumer protection investigation of direct mail and telemarketing schemes, Mar. 3, 2005, available at http://www.state.ia.us/government/ag/latest_news/releases/mar_2005/Walter_Karl.html.

¹⁴⁹ Affidavit of Barbara Blake, Investigator, Office of the Attorney General of Iowa, Mar. 1, 2005, available at http://www.state.ia.us/government/ag/latest_news/releases/mar_2005/Walter%20Karl%20Blake%20Affidavit%203-1-05.pdf.

¹⁵⁰ 15 USC § 6101.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). This law explicitly allows spamming; companies can send spam on an opt-out basis. CAN-SPAM codifies the opt-out requirement, sets rules for its implementation, and requires disclosures of the sponsors of the spam. Junk faxes are regulated by the Telephone Consumer Protection Act, and require opt-in consent for transmission. Violators of the Act can be sued in small claims court for \$500 a fax.

Third party (advertiser) liability is an important feature of direct marketing regulation. Improper supervision of calling centers or spamming companies can result in liability for the sponsor of the advertisement. For liability to occur, CAN-SPAM requires that the advertiser have knowledge of the spamming, benefit from it financially, and not take action to end the spam.¹⁵¹ In the telemarketing context, FTC rules impose advertiser liability where third parties, “provide substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any [prohibited] act or practice...”¹⁵² Junk faxes can trigger liability where fax broadcasters, “demonstrate[] a high degree of involvement in, or actual notice of, the unlawful activity and fail[] to take steps to prevent such facsimile transmissions.”¹⁵³ Advertisers hiring fax broadcasters are directly liable for their activities.

The challenge in remedying direct marketing violations almost always relates to the tracing the provenance of the communication. Telemarketers are known to hang up when consumers object to a call or demand information about their business. Junk faxes obfuscate the origin of their communications. Spammers can easily mask the origin of their communications. Collective action problems stop consumers from taking the steps necessary to trace the provenance of these communications. Telemarketers and junk faxers can use “boiler rooms” that are easily moved once complaints begin to amass with regulators. The advent of VOIP makes telemarketing and junk fax broadcasting highly portable and difficult to trace. Regulators generally act reactively, sometimes years after a huge nuisance begins to operate.¹⁵⁴ This series of challenges has caused some states to impose bond requirements on telemarketers. But advertiser liability as an additional approach can produce incentives to prevent the hiring of firms that engage in illegal direct marketing practices.

In person solicitation at the home can be blocked through the posting of a “no solicitation” sign,¹⁵⁵ and in some cases, is subject to “cooling off” periods that allow the consumer to cancel a transaction without penalty.

Advertising mail (junk mail) is unregulated on privacy grounds,¹⁵⁶ and consumers can only employ self-regulatory systems to reduce its volume. The Direct Marketing Association has revamped its website to assist individuals in opting out from advertising mail.¹⁵⁷ Consumers

¹⁵¹ 15 USC § 7705.

¹⁵² 16 C.F.R. § 310.3(b).

¹⁵³ 47 C.F.R. § 64.1200(a)(3)(vii).

¹⁵⁴ Notorious junk faxer Fax.com operated for years before attracting effective regulatory attention. *See* Ryan Singel, *Curtain Call for Junk-Fax Blaster*, *Wired*, Oct. 9, 2004.

¹⁵⁵ *Rowan v. Post Office Dept.*, 397 U.S. 728 (1970).

¹⁵⁶ Some consumers have used 39 USC § 3008 to block junk mail. This statute allows consumers to block mail on a sender-by-sender basis, on the allegation that the mail is pornographic. This determination is based entirely on the subjective perception of the consumer. But the process is laborious and can only be accomplished offline, by sending the mailpiece to the postal service.

¹⁵⁷ See <https://www.dmachoice.org/>

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

report that enrolling in the DMA’s mail preference service results in a substantial decrease in advertising mail volume. However, several problems remain: the service is not well known, it only applies to DMA members that must pay a fee for membership and access to the suppression list, and the most marginal actors in the advertising mail business are not likely to honor individuals’ privacy preferences. This last problem is likely to grow in intensity as the population of the US ages.¹⁵⁸

Credit reporting

The first US federal privacy law addressed credit reporting. The Fair Credit Reporting Act of 1970 provides individuals with access to and correction rights for consumer reports, limits disclosure of reports to individuals with a legitimate interest, and encourages a higher level of professionalism and accountability in the credit reporting field.¹⁵⁹ More recent amendments give individuals a right to obtain a free copy of their consumer report from each nationally-operating consumer reporting agency, to block information accrued from identity theft incidents, and to access business records generated by identity theft impostors. The FCRA regulates traditional credit reporting, but also tenant screening (for rental housing), and employment background screening.

Four high level principles of the FCRA are important to consider. First, credit reporting is not consent based. Every credit-active American is likely to have a file in the nation’s major credit reporting databases, operated by Innovis, Experian, Equifax, and Trans Union. Individuals cannot opt out of credit reporting.

Second, in exchange for this non-consensual system, consumer reporting agencies are subject to accuracy standards. The FCRA requires consumer reporting agencies to follow reasonable procedures to assure maximum possible accuracy of the information pertaining to an individual. This is an evolving standard that recognizes that over time, procedures to ensure accuracy could improve. But it also recognizes that consumer reporting will never be perfectly accurate. Consumer reporting agencies thus are largely immune for actions of defamation.

Third, in the US, credit reporting covers both positive and negative information. Incentives are set such that companies routinely furnish positive payment information to consumer reporting agencies on consumers. Conversely, companies also use the system to report negative information, because such derogatory information causes many consumers to resolve unpaid bills and debts.

Fourth, credit reporting laws govern the extension of credit, but also tenant screening and background checks for employment purposes. The FCRA applies in tenant screening and background checks only when the decision maker hires a service to obtain a consumer report. Thus, a landlord or employer who does the check herself does not trigger the FCRA, even when searching public records or the internet for positive or derogatory information about an individual. This is a major loophole that was sensible in the pre-internet era, but now

¹⁵⁸ Karen Blumenthal, How Banks, Marketers Aid Scams, Wall Street Journal, Jul. 1, 2009 (“Another eye-opener was how quickly our [elderly] relative’s phone calls and mail increased once he began replying to sweepstakes and lottery offers. Law-enforcement officials say his response likely landed him on so-called sucker lists that were repeatedly sold.”).

¹⁵⁹ 15 USC § 1681 et seq.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

presents increasing problems. An employer could perform a web search for a prospective applicant and reject her, because of derogatory information available on the web. In that situation, the employer would not need to give the employee notice, would not need to verify the accuracy of the information, nor would need to confirm that the derogatory information pertained to the applicant. Similarly, background checks done for non-employment purposes, such as volunteer screening, or for other private investigation purposes may not be covered by the FCRA.

The Commercial Data Broker

Much US privacy law addresses the annoyance of direct marketing activities, but completely ignores issues of data collection and processing that enabled the direct marketing contact. For instance, the telemarketing and spam laws do not create substantive rights in data, but rather restrict how companies can contact individuals. Great attention is paid to the annoyance of persistent marketing, and to identity theft, while more subtle problems of information collection and use remain unaddressed.

The inattention to collection and use have led to some of the country's most serious privacy challenges. The sectoral nature of the US system exposes the greatest weaknesses in contexts where there is no business relationship between the individual and the business. One such example is the "commercial data broker."

While a comprehensive regulatory system creates rights in consumer reports used for employment, tenancy, and for credit granting, a wide spectrum of business practices fall outside the Fair Credit Reporting Act. Non-FCRA covered "commercial data brokers" sell information that is similar to that in regulated consumer reports, but they do so for unregulated purposes, such as authentication, risk assessment, investigations, and the like. In some cases, consumer reporting agencies themselves operate parallel data broker businesses outside the FCRA.

Commercial data brokers have become a major source of personal information for law enforcement and intelligence agencies.¹⁶⁰ In effect, these companies have allowed the US government to circumvent Privacy Act prohibitions on the creation of a personal information clearinghouse. Law enforcement has become so dependent upon these services that the FTC intervened in a recent merger of two data brokers to prevent prices for government access from rising.¹⁶¹

The rise of commercial data brokers is another example of the failure of self-regulation to police private-sector activity. In the 1990s, privacy advocates warned the public about the risks to privacy that were posed by direct marketers. In response to this criticism, the Direct Marketing Association (DMA), touted its self-regulatory ethical guidelines. Article 32 of the guidelines specifies, "Marketing data should be used only for marketing purposes."¹⁶² In numerous representations to the media and regulators, DMA officials and direct marketers

¹⁶⁰ Chris Jay Hoofnagle, Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement, 29 N.C.J. Int'l L. & Com. Reg. 595 (2004).

¹⁶¹ Federal Trade Commission, FTC Challenges Reed Elsevier's Proposed \$4.1 Billion Acquisition of ChoicePoint, Inc. To Preserve Competition, Order Requires Divestiture of Assets Related to ChoicePoint's AutoTrackXP and CLEAR Electronic Public Records Services, September 16, 2008, available at <http://www.ftc.gov/opa/2008/09/choicepoint.shtm>.

¹⁶² Available at <http://www.dmaresponsibility.org/Guidelines/>.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

attempted to quell criticism surrounding the possibility of law enforcement access to marketing data."¹⁶³

In 1997, the DMA renewed this promise, stating in a filing to the Federal Trade Commission that: “The Direct Marketing Association has long had a policy opposing the use of personal data obtained from marketing transactions for non-marketing purposes. Our Guidelines therefore limit the sources of the information used by look-up services. Companies that maintain databases of both marketing and non-marketing information ensure that information gained from marketing transactions is not used as an information source for the look-up database.”¹⁶⁴ Nevertheless, many commercial data brokers are marketing companies; several are DMA members. The targeting science fostered in an unregulated direct marketing industry was ported over to citizen targeting and transparency with alacrity.

Identity information

Identity information is not explicitly regulated in the US, except to the extent that fraud using identification information of another is illegal.

Because of the sectoral nature of US privacy protections, companies that are in the position to collect identification information are free to aggregate it and sell it, even when the same information would be highly protected under US law in similar contexts. For instance, individuals’ driver records are strongly protected by the Drivers Privacy Protection Act. However, companies are free to collect this same information from the face of drivers licenses in the many situations where they are required for access to a product or service. A car rental company is free to scan drivers licenses, collect the information from them (including the “highly sensitive” photograph of the driver), and amass a database for its own use or for sale to others. An automotive service company would be free to collect license plate and VINs of its customers’ cars and resell them to private investigators. In most states, a bar is free to scan drivers licenses for the purpose of verifying age, and then repurpose the data for marketing.¹⁶⁵

The Use of Publicly Accessible Data (‘Public Registers’)

There are several different types of records held by the government that are subject to varied access provisions.¹⁶⁶ “Agency records” held by federal agencies can be requested under the

¹⁶³ A Matter Of Privacy, Delaney Rep. (Informed Communications, Inc., New York, New York), Vol. 4, No. 34 (Aug. 30, 1994), available at 1993 WL 2870174.

¹⁶⁴ The DMA did reserve the right to use public records for any purpose. See Direct Mktg. Ass'n, Written Comments of The Direct Marketing Association Before the Federal Trade Commission (Apr. 15, 1997) (FTC Docket Nos. Database Study P974806, Consumer Privacy P954807) available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/dma.htm>.

¹⁶⁵ Jennifer 8. Lee, Finding Pay Dirt in Scannable Driver's Licenses, New York Times, Mar. 21, 2002. (About 10,000 people a week go to The Rack, a bar in Boston...One by one, they hand over their driver's licenses to a doorman, who swipes them through a sleek black machine... Mr. Barclay bought the machine to keep out underage drinkers who use fake ID's. But he soon found that he could build a database of personal information, providing an intimate perspective on his clientele that can be useful in marketing. "It's not just an ID check," he said. "It's a tool.").

¹⁶⁶ For an authoritative and in-depth discussion of this issue, see Daniel Solove, Access and Aggregation: Privacy, Public Records, and the Constitution, 86 Minnesota Law Review 1137 (2002), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=283924.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

Freedom of Information Act. However, personal information in those records are usually redacted pursuant to two different exemptions that justify withholding such information.¹⁶⁷

Governments also maintain “public records.” While the scope of public records varies on a state by state basis, generally speaking court records, property records, arrest and conviction records, and business registration records are public. Public records are open to inspection by any person, and clerks responsible for such information generally do not require individuals to identify themselves or the purposes for which they wish to use public records. Increasingly, public records are available online to anyone. Additionally, many authorities responsible for public records will make the entire database available to commercial data brokers for a fee.

Information in public records, generally speaking, can be used for *any* purpose. Once information is disclosed in a public record, that information ceases to be private, and thus eliminating the ability under the privacy torts to sue for further revelation of the information. Companies are free to aggregate, repurpose, and commercialize personal information in public records.

An individual arrested in a state such as Florida is likely to have their mug shot broadcast to the world,¹⁶⁸ and specialized websites collect these images (especially those of pretty women) for amusement.¹⁶⁹ Those arrested may not be guilty of any crime. Yet their pictures, including photographs of tattoos and scars, are placed on the internet by the government for anyone to use for any purpose.¹⁷⁰

With the growth of government involvement in individuals’ lives, an increasing amount of personal information appears in public records. This trend, along with the struggle for a transparent government has resulted in a transparency citizenry.

One attempt to impose use limitations was implemented by the City of Los Angeles. That city only released arrest information to the public for specific purposes, including law enforcement, research, and journalistic uses. Commercial resale of the information was restricted.¹⁷¹ The Los Angeles approach is an exception not followed by many jurisdictions.

The Internet

The US still lacks a broadly-applicable law regulating collection of personal information online. In 2003, the US Congress passed the Children’s Online Privacy Protection Act (COPPA), which makes it an unfair or deceptive trade practice to knowingly collect the personal information of children (defined as individuals under the age of 13) without parental consent. Internet privacy is largely governed by Federal Trade Commission precedent, summarized above in section 3.

¹⁶⁷ 5 U.S.C. § 552(b)(6), (7).

¹⁶⁸ See e.g. <http://www.sarasotasheriff.org/arrests.asp>

¹⁶⁹ See e.g. <http://www.mugshots.com> .

¹⁷⁰ See e.g. Miss Mug Shot Florida, Is it wrong to say we look forward to her next arrest?, Jan. 15, 2008, available at <http://www.thesmokinggun.com/archive/years/2008/0115083array1.html> .

¹⁷¹ LAPD v. United Reporting, 528 U.S. 32 (1999)

8. Cross-Border Data Transfers

Transfers into USA (Outsourcing practices)

The US Department of Commerce has negotiated a “safe harbor” agreement to meet the EU Data Protection Directive’s “adequacy” requirement for data transfers to the US. Under this safe harbor, US companies can voluntarily certify compliance with a set of principles; in exchange, these companies are subject to enforcement actions of the FTC instead of European authorities.

Transfers out of USA (Data exports)

US privacy law has not explicitly addressed the issue of “offshoring.” There has been a growing public awareness of offshoring data processing activities to India, Pakistan, the Philippines, and elsewhere. When this first came to public light industries involved were extremely secretive about the practice generally, but in subsequent years, a number of data-intensive industries moved data processing or customer service to other countries. Despite several salient examples of offshore data being misused, legislation to address the practice has been introduced but not passed.

Nevertheless, offshoring of US data could be said to be regulated in at least four ways: first, technical measures were introduced by offshoring entities to reduce the risk that employees could copy personal information. For instance, call centers would not allow employees to enter with pens or paper.

Second, and consistent with the US sectoral approach, at least three recently enacted US privacy laws require companies using business partners or service providers to have reasonable privacy or security protections. Under the Health Insurance Portability and Accountability Act, covered entities with personal information must gain assurances of confidentiality from other businesses. This is done with a “businesses associate contract.” Similarly, the Gramm-Leach-Bliley Act, which regulated financial services organizations, created obligations to oversee service providers and incorporate the use of outside entities into a security safeguards plan. A number of guidance documents released by financial services regulators further specifies risk mitigation in outsourcing/offshoring/third party contracts. In the tax preparation context, an recently promulgated IRS rule now allows US businesses to share Social Security numbers with non-US firms, with notice and consent of the data subject, along with adequate security safeguards.

Third, security breach notification laws require companies to notify individuals when personal information was accessed by an unauthorized person. If the data in question were held by a service provider, assuming compliance with these notification laws, the offshore service provider would inform the company of the breach, which in turn, would notify consumers and regulators.

Fourth, public perception regulates the use of offshoring. In a salient early example, a sub-sub-contractor of a medical firm in the US threatened to publicly release information on the firm’s patients, if payment was not received for transcription services performed. This type of incident can have permanent effects on the practical ability of firms to offshore.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

There are several consumer protection problems in offshoring. First, if offshoring is present in a business relationship, it is unlikely to be explicitly disclosed to the data subject. For instance, in the financial services context, notice would be effectuated by stating that the bank may transfer personal information to a service provider.¹⁷² Service providers train their call center employees to mask their location and to affect western accents.

Of course, notice is just one aspect of fairness to data subjects. Even with notice, consumers may not be able to fairly judge an offshoring opportunity as more safe or desirable than processing in the US. Key rights to enable this decision making are lacking--there is no right to access or audit these relationships. In the event of harm to the consumer, in both the GLBA and HIPAA contexts, there is no private right of action. Thus, the consumer is limited to filing complaints with regulatory agencies.

Finally, it is important to note that the protections that do exist apply to only a few sectors—tax preparation, health care, and financial services. Little is publicly known about offshoring outside these contexts (such as credit reporting), what technical safeguards are in place, what the track record for breaches is, etc. US privacy law is so limited that even if problems existed in the space, it would be difficult for consumers or regulators to identify and remedy them.

9. Rights of Data Subjects

Because the US follows a sectoral model, these sections will contain examples of how US privacy law incorporates fair information practices.

Informing of Data Subjects

There is no general obligation among companies to inform individuals of data collection, use or disclosure. In certain sectors, notice is required.

In the online context, websites generally are required to post a privacy policy to inform individuals of information practices. This requirement is imposed by California state law, which requires operators of commercial web sites to post privacy policies and adhere to representations made.¹⁷³ This privacy policy must identify the categories of personally identifiable information that the operator collects, the categories of third-party persons or entities with whom the operator may share that personally identifiable information, and provide information about access and correction, if the company maintains processes for those rights. Additionally, the policy must notify individuals of the effective date of the policy, and how changes to the policy will be communicated. Technically, a company that did no business with California residents could ignore these requirements, but the California market is so lucrative that the law is essentially a national mandate.

¹⁷² E-Loan is a notable exception to this statement. The company offers its customers the choice to offshore loan information to India for faster processing, or to have the processing performed in the US more slowly. John Lancaster, *Outsourcing Delivers Hope to India Young College Graduates See More Options for Better Life*, Washington Post, May 8, 2004, at A1.

¹⁷³ Cal. Bus. & Prof. Code § 22575.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

Federal privacy law requires financial institutions (banks, insurance companies, and brokerages), cable service providers, and certain other businesses to provide privacy notices to individuals. These notices are typically provided annually.

However, the average business operating offline can collect, use, and disclose personal information without a privacy policy. Thus, most US bricks-and-mortar retailers do not have privacy policies at the cash register, despite common practices among retailers of sharing data with third parties and engagement in cooperative data sharing arrangements. Companies regularly engage in schemes where personal information is collected for some third party marketing purposes without explicit disclosure to the consumer (sweepstakes, product warranty registration cards, etc).

Under a unique California law, state residents may request that companies disclose the identities of their third party marketing partners, and may opt out of information sharing with these third parties.¹⁷⁴

Confirmation of processing

US privacy law does not generally recognize a right to demand confirmation of data processing. Individuals interested in processing of personal information would typically use access provisions to confirm that a company possessed data.

Access

Several US privacy laws subject certain sectors to access responsibilities. Most notably, the FCRA requires consumer reporting agencies to disclose “all information in the consumer’s file at the time of the request...”¹⁷⁵ However, this same provision explicitly allows consumer reporting agencies not to disclose credit scores, which are increasingly important in credit-granting decisions.

Access rights in the credit reporting context are further complicated by the use of the word “file,” which was adequate when the law was enacted in 1970, but no longer relevant today. The consumer reporting agencies produce a “file” based upon the terms of a request to their systems. Thus, a narrow request for an individual that includes their Social Security number and date of birth may return a thinner “file” than a search that used fewer terms.

Access provisions are also present in the Cable Communications Policy Act. This allows consumers to request all personally identifiable information maintained by a cable service provider.¹⁷⁶ This request must be done in person.

Privacy Act contains an access provision that is usually employed in combination with the Freedom of Information Act. These laws can be used to obtain personal information in federal executive agency records.

¹⁷⁴ Cal. Civ. Code. § 1798.83.

¹⁷⁵ 15 USC 1681(g).

¹⁷⁶ 47 USC § 552 (d).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

Correction

The most robust correction rights governing the private sector are present in the Fair Credit Reporting Act, and are described in section 4.4 above.

The Cable Communications Policy Act requires that subscribers can access personal information, after making an in-person request. It further requires that, “A cable subscriber shall be provided reasonable opportunity to correct any error in such information.”¹⁷⁷

Notification of disclosure

US privacy law requires notification of disclosure of information in some contexts. In most cases, individuals are not notified of disclosures unless they ask for an accounting of them. The Fair Credit Reporting Act requires consumer reporting agencies to maintain a log of companies that access an individual’s consumer report, and to disclose this list to the individual when a consumer report is requested.¹⁷⁸ Thus, consumers can determine whether parties outside the consumer reporting agency obtained their report, and potentially pursue privacy claims against them. However, despite the efficiencies of internet and new wireless communication technologies, consumer reporting agencies do not proactively notify consumers of third party access (except in situations where consumers have purchased credit monitoring services).

The Health Insurance Portability and Accountability Act requires health care providers to maintain an audit log.¹⁷⁹ This auditing requirement has unearthed and substantiated the problem of unauthorized “browsing” of files. As a result of a California law requiring notice of unauthorized access to medical information, 823 breaches were reported to a state agency covering the time period of January to July 2009.¹⁸⁰ The California laws were motivated by concerns that tabloid newspapers were paying file clerks to leak information,¹⁸¹ because some employees were browsing to satisfy their own curiosity, and because of concerns that health care facilities were using the information for their own marketing purposes.

Right to object to direct marketing

Congress has “split the baby” on default rules for direct marketing. Statutes tend to have a mixture of both opt-in and opt-out protections. For instance, the FCRA requires affirmative consent (opt-in) for access to a consumer’s report. However, consumer reporting agencies are free to assemble mailing lists of consumers who qualify for certain offers of credit on an opt out basis. This practice, called prescreening, allows a marketer to purchase a list of individuals who meet some criteria for a financial product.

¹⁷⁷ 47 USC § 551(d).

¹⁷⁸ 15 USC § 1681g(a)(3).

¹⁷⁹ 45 CFR § 164.312(b).

¹⁸⁰ Joyce E. Cutler, Over 800 Breaches of Patient Information Reported to California Officials Since January, 8 Privacy and Security Law Report 1053, Jul. 20, 2009.

¹⁸¹ “...The tabloid [National Enquirer] deposited checks totaling at least \$4,600 into her husband's checking account beginning in 2006, prosecutors said...Jackson and state officials have disclosed that records for Spears, Fawcett and California first lady Maria Shriver were among those breached.” Former UCLA hospital worker admits selling celeb medical records, Dec. 1, 2008, available at http://www.usatoday.com/life/people/2008-12-01-UCLA-records_N.htm.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

Similarly, the Cable Communications Policy Act prohibits revelation of cable viewing behavior without opt-in consent. But the same law allows cable service providers to generate mailing lists of their customers for sale to others on an opt-out basis.

Educational records cannot be viewed, except for certain purposes, without the student's consent. However, the FERPA allows for disclosure (and sale) of "directory information" on an opt out basis. This includes: name, address, phone number, email address, dates of attendance, degrees awarded, enrolment status, and major field of study. An even broader range of information is released about athletes.

Telemarketing to wireless phones requires opt-in consent, but the same calls to a landline telephone are governed by opt-out rules. The sale of phone calling records (non-content CPNI) was recently switched from an opt out to an opt in standard. Email marketing is governed on an opt out basis.

Sometimes these compromises result in compromised privacy. For instance, under the Video Privacy Protection Act, videotape rental companies are not to release the names of movies and other materials rented by customers. However, these companies may assemble genre lists (e.g. Customer John Doe watches adult films) and sell them to third party marketers on an opt-out basis.

In more recent years, the US Congress has legislated with a trend towards opt-out rules. Recently enacted laws regulated financial services (opt-out for information sharing among third parties) and commercial email (opt out).

In some circumstances, there is "no opt." A wide variety of companies that lack a relationship with consumers remain largely unregulated by statutory privacy law. "Commercial data brokers," for instance, may adhere to self-regulatory standards, but otherwise are not under statutory duties to give individuals notice, access to data, or the ability to opt out of information sharing. The most notable example of "no opt" comes from the FCRA: consumers cannot opt out of credit reporting. In 1970, Congress struck a bargain with consumer reporting agencies, allowing these companies to assemble files on consumer with broad immunity from suit so long as they maintain procedures to ensure "maximum possible accuracy" in consumer reports.

Perhaps the most compelling evidence of Americans' support for limits on third party information sharing is from North Dakota. That State's legislature switched the default standard for sharing financial information from opt-in to opt-out. A referendum was organized, and in June 2002, 73% rejected the legislature's dilution of privacy rights, and voted to reestablish an affirmative consent standard for banks that wished to sell personal information to others.¹⁸²

¹⁸² NORTH DAKOTA SECRETARY OF STATE, STATEWIDE ELECTION RESULTS, Jun. 11, 2002, available at <http://web.apps.state.nd.us/sec/emspub/gp/electionresultssearch.htm?displayCode=MEASURE&cmd=Search&officeElectionNo=All+Offices+and+Measures&searchType=STATE&electionDate=06112002&showMap=N&resultType=All+Offices+and+Measures>.

10. Individual Remedies

Privacy remedies are particularly problematic in the US. American courts are skeptical of laws that impose fines for a mere violation of a statute. It seems inequitable to impose a fine upon a company for a mere technical violation of a complex statute, untethered to some form of “harm.” For instance, the Supreme Court recently held that damages under the Privacy Act of 1974 require a showing of “actual damages” to order to obtain a money damage recovery.¹⁸³

“Actual damages” too, is a problem. US courts, generally, do not view invasions of information privacy as some assault to inviolable personality rights.¹⁸⁴ Instead, courts tend to read a common law “harm” requirement into privacy statutes, even when those laws call for recovery absent a showing of actual damages. In the US, special attention is paid to economic damages. For instance, despite the announcement of major security breaches by many different companies in recent years, victims of these breaches have been unsuccessful in the courts. Courts have held that the breach and the mere risk of increased identity theft do not constitute legally-cognizable harms.¹⁸⁵

The Supreme Court is clearly developing a substantive due process right to be free of exorbitant damage awards in lawsuits.¹⁸⁶ If extended to statutory law, certain privacy statutes are likely to become more difficult to enforce. Some privacy statutes, such as the Drivers Privacy Protection Act, which set a \$2500 damage award per violation, combined with the practice of buying entire motor vehicle databases, can quickly amount to billion-dollar liability. Thus, damage awards in information privacy lawsuits, lacking harm, and keyed to a technical violation of a statute, are likely to be viewed with skepticism. Congress is likely to have to grapple with this issue in passing new privacy legislation.

Most federal privacy laws have liquidated damages provisions. As mentioned earlier, the Supreme Court has interpreted the Privacy Act to require actual damages in order to invoke the Act’s liquidated damage provision of \$1,000.

The Fair Credit Reporting Act imposes different levels of liability depending upon whether the violation was willful or negligent. In either case, plaintiffs can obtain costs and attorney’s fees.¹⁸⁷

The Video Privacy Protection Act provides for \$2,500 in liquidated damages, punitive damages, attorneys fees and costs, and preliminary and equitable relief.¹⁸⁸

The Cable Communications Protection Act grant liquidated damages of \$100 per violation per day, or \$1000 (whichever is higher), and attorney’s fees and costs.¹⁸⁹

¹⁸³ Doe v. Chao, 540 U.S. 614 (2004).

¹⁸⁴ In cases of defamation and physical invasions of privacy, US courts are more likely to recognize emotional distress and non-economic harms.

¹⁸⁵ Pisciotta v. Old National Bancorp, 449 F.3d 629 (7th Cir. 2007).

¹⁸⁶ See e.g., BMW v. Gore, 517 U.S. 559 (1996).

¹⁸⁷ 15 USC § 1681n, 1681o.

¹⁸⁸ 18 USC 2710 (c).

¹⁸⁹ 47 USC § 551(f).

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

One of the most successful individual remedies provisions is found in the Telephone Consumer Protection Act of 1991.¹⁹⁰ That law allows many consumers to sue in small claims court to remedy unwanted telemarketing, instead of federal court. The barriers to enforcement are much lower in small claims court, and are navigable by ordinary consumers. Consumers can obtain \$500 a violation, or where the telemarketer acted willfully or knowingly, \$1,500 per violation.

But statutes calling for liquidated damages are largely the product of 1970s and 1980s interventions. The recent trend is to provide no private right of action at all, and to vest enforcement in public agencies. The Children’s Online Privacy Protection Act of 1998 specifies that violations “shall be enforced by the [Federal Trade] Commission.”¹⁹¹ Similarly, the Gramm Leach Bliley Act entrusts enforcement to federal regulatory agencies.¹⁹²

An exception to this trend is the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). That law vested enforcement in government agencies, but also granted a right of action to providers of internet access providers.¹⁹³

11. Supervision, Notification and Enforcement

The US lacks a data protection commissioner, or other similar official responsible for information privacy broadly. In 1999, the Clinton Administration created a chief counsel for privacy position in the Office of Management and Budget, but that position was not recreated in the Bush and Obama Administrations.

12. Sectoral (Self-) Regulation and Codes of Conduct

The role of the FTC (1): general support for self-regulation

The Federal Trade Commission has maintained a pro-self-regulatory approach for most of its history of overseeing internet practices. At the FTC’s 2005 hearings on consumer protection online, the FTC concluded that the essential elements of a balanced consumer protection program are:

- Coordinated law enforcement by state and federal agencies against fraud and deception;
- Industry self-regulation and private initiatives to protect consumers; and
- Consumer education through the combined efforts of government, business, and consumer groups.¹⁹⁴

¹⁹⁰ 47 USC § 221(b)(3).

¹⁹¹ 15 USC § 6505(a).

¹⁹² 15 USC § 6805.

¹⁹³ 15 USC § 7704(g).

¹⁹⁴ Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (hearing report, May 1996): 46 (formatting added). Also available online at http://www.ftc.gov/opp/global/report/gc_v2.pdf.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

The report continued:

The hearing record is replete with examples of private initiatives: industry self-regulation programs and plans to develop and expand such programs, technology-based consumer protections and self-help opportunities, and commitments to undertake new consumer education programs. These and other initiatives will be crucial in providing consumer protection in the new marketplace.¹⁹⁵

Over the past ten years, the FTC has pursued these three goals. It has brought an impressive array of actions under the agency's authority to prosecute unfair or deceptive trade practices.¹⁹⁶ It has fostered self-regulatory programs and it continues to operate multilingual consumer outreach both online and offline.

Nevertheless, several salient limitations are present in the FTC's approach.

First, self-regulation has to be conceived of as a form of regulation; it is often developed as an alternative to legal regulation. As such, it often is weaker than what might be obtained in a legislative bargain (see discussion below).

Second, while the FTC has been successful in enforcing promises made in privacy policies, individuals have been unsuccessful in enforcing similar representations. The first cases to look at the legal status of privacy policies concluded that they were not binding contracts, but rather policy statements.¹⁹⁷ Thus, self-regulatory regimes are practically unenforceable by individuals, meaning that the risk of agency "capture" is heightened in self-regulatory regimes.

Third, the damages that the FTC receives from actions may be less than what the company made in actual fraud. For instance, in the Adteractive case, the company settled with the FTC and agreed to pay \$650,000 in civil penalties for alleged deceptive advertising practices, when the company reported annual revenues exceeding \$115 million.¹⁹⁸ Similarly, in the DirectRevenue case, the FTC settled for \$1.5 million for a business practice that gained the company \$20 million in investment revenue.¹⁹⁹

We will return to the role of the FTC later, but now first consider the most important industry bodies involved in self-regulation.

¹⁹⁵ Id.

¹⁹⁶ Marcia Hoffman, "Federal Trade Commission Enforcement of Privacy," in *Proskauer on Privacy* (New York: Practising Law Institute, 2006).

¹⁹⁷ See *In Re Northwest Airlines Privacy Litigation*, 2004 WL 1278459 (D. Minn. 2004); *Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196 (D.N.D. 2004).

¹⁹⁸ "Whether or not the \$650,000 penalty Adteractive agreed to pay is harsh enough to deter similar violations also is up for debate. Of the five commissioners voting on the settlement decision, one dissented on grounds that the civil penalty is "inadequate." In his dissenting statement, Commissioner Jon Leibowitz referenced Adteractive's reported annual revenues of over \$115 million, citing a 2005 San Francisco Business Times article. Industry observers agree the firm, founded in 2000, was making around \$100 million annually by 2005, and a former employee told ClickZ News last month the company was valued at more than \$400 million when business was booming." Kate Kaye, *FTC Settlement with Adteractive Leaves Unanswered Questions for Troubled Firm*, ClickZ News, Nov. 29, 2007, available at <http://www.clickz.com/3627728>.

¹⁹⁹ Jason Lee Miller, *DirectRevenue Slapped (Lightly) By FTC*, Feb. 21, 2007, available at <http://www.webpronews.com/topnews/2007/02/21/directrevenue-slapped-lightly-by-ftc>.

Industry bodies

The Network Advertising Initiative

The Network Advertising Initiative (NAI) is one of two major self-regulatory initiatives covered here. As network advertisers, companies such as DoubleClick that track individuals as they navigate the web, came under greater scrutiny for privacy problems, the NAI proposed a set of self-regulatory guidelines. These July 2000 guidelines encompassed only notice, opt-out, and "reasonable" security. NAI members could transfer information amongst themselves to an unlimited degree, so long as it is used for advertising. No meaningful enforcement mechanism or access rights were incorporated.

The opt out fashioned by the NAI agreement was cookie based. The requirement to download a NAI opt out cookie contravened common privacy practices—many advised consumers to delete their cookies to prevent tracking, but deleting the NAI cookie would undo that privacy-enhancing step.

The scope of opt out was also very limited. Opting out did not mean that NAI entities would stop tracking consumers. Instead, it meant that consumers would not receive targeted advertisements. This seems to be the privacy worst case scenario: the privacy problem (tracking across sites) is preserved, but the privacy-sensitive consumer ends up opting out of the putative benefit of the tracking (targeted advertising).

In a 2007 report on the NAI, privacy research Pam Dixon noted that the organization created a "associate membership" in 2002, to include companies that were not fully in compliance with these limited protections.²⁰⁰ By 2005, these associate members outnumbered full-compliance members. The self-regulatory body charged with monitoring and ensuring compliance with the principles, TRUSTe, engaged in inconsistent and spotty reporting, and there is no evidence of promised "random audits" of NAI members.²⁰¹

IRSG

The Individual Reference Services Group (IRSG) Principles were developed by commercial data brokers in the late 1990s in order to preserve the sale of Social Security numbers free of statutory restriction. IRSG members sold SSNs and other personal information to marketers, insurers, private investigators, landlords, and law enforcement.

Like the NAI, the IRSG Principles set forth a weak framework of protections. They allowed companies to sell non-public personal information "without restriction" to "qualified subscribers." The problem with this approach later became clear—IRSG members themselves were to determine who was qualified.

Under the IRSG Principles, individuals can only opt-out of the sale of personal information to the "general public," but commercial data brokers don't consider any of their customers to be members of the general public.

²⁰⁰ Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*, Fall 2007, available at http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

²⁰¹ *Id.*

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

Privacy seals and certifications

Privacy seals represent some third-party certification of a web site's privacy practices. In the past ten years, a number of seal programs have emerged, with some focusing on privacy and others certifying compliance with some standard for site security. There are no legislative or regulatory standards for seal programs, and thus, consumers may be confused about the actual protections in place. Researcher Chris Connolly wrote in 2008 that:

Some trustmark schemes make very little attempt to impose privacy standards. Trust Guard Privacy Verified seal looks impressive to consumers, but to qualify you only have to include a brief three paragraph privacy policy.

Trust Guard also promises that 'As soon as you place your Multi-Seal order, we'll begin the verification process, send you your Seals, and set up your Certificate within one business day; updating any outstanding issues on your Certificate as they are verified. This allows you to start receiving benefits to your website right away!' The cost of the privacy seal is either \$197 per year or about \$130 per year as part of a multi-seal package deal. Readers may wish to make their own determination of the level of privacy protection provided by Trust Guard at these prices when combined with their 24 hour approval process.²⁰²

In the privacy field, TRUSTe²⁰³ is the most popular privacy seal program. Its main competitor in the privacy space, the Better Business Bureau (BBB), no longer issues privacy-specific seals, and instead offers a broader program for its members. The BBB's broad seal makes only basic privacy requirements, many of which are already required by California and federal law.²⁰⁴ For instance, the BBB seal requires that companies post a privacy policy and abide by it; it also allows businesses to send unsolicited commercial email, so long as they offer an opt out right. Under these guidelines, BBB would certify a company that sells customer information to third parties on an opt out standard. This is problematic because, as noted above, most US consumers believe that a website with a privacy policy does not sell data to third parties.²⁰⁵ Consumers would rationally assume that a website with both a privacy policy and a seal would have even more stringent protections.

Similarly, TRUSTe's general web privacy requirements do not set stringent substantive limits on website practices. The primary protection is a requirement for a privacy policy, and to abide by its terms. Like BBB, TRUSTe allows sale of consumer personal information to third parties on an opt-out basis.²⁰⁶

²⁰² Chris Connolly, Trustmark Schemes Struggle to Protect Privacy (2008), available at http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/.

²⁰³ Disclosure: The author is a member of TRUSTe's Advisory Board.

²⁰⁴ Better Business Bureau, BBBO nLine Code of Online Business Practices Final Version, n.d., available at <http://www.bbbonline.org/reliability/code/principle3.asp>

²⁰⁵ Turow, Joseph, Americans & Online Privacy, The System is Broken, Annenberg Public Policy Center, June 2003, available at http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf; Joseph Turow, Lauren Feldman, & Kimberly Meltzer, Open to Exploitation: American Shoppers Online and Offline, Annenberg Public Policy Center of the University of Pennsylvania, Jun. 1, 2005.

²⁰⁶ TRUSTe, Program Requirements, n.d., available at <http://www.truste.org/requirements.php>

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

TRUSTe requires member sites to undergo a review, which includes an assessment to determine whether a company abides by whatever promises are made in its privacy policy. TRUSTe incorporates notice, access, choice, and security mechanisms in its requirements for certified sites. However, the company has been reluctant to report violators to authorities. Almost without exception, complaints are resolved through informal mechanisms.

Instead of substantive limits on practices, TRUSTe offers consumers a guarantee that there will be a forum for complaints, and an attempt to resolve complaints. The results of this complaint process are now made publicly available;²⁰⁷ in fiscal year 2008, TRUSTe received over 4,700 complaints (almost half of which concerned websites that used the TRUSTe seal without permission) and terminated 4 members.²⁰⁸

Privacy seal programs suffer from a fundamental incentive problem: some companies that have a strong user base have few incentives to have their privacy practices certified. For instance, Google and MySpace do not have TRUSTe privacy seals. At the other end of the spectrum, more marginal websites that seek a larger user base have strong incentives to be certified. TRUSTe and other seal programs gain revenue from issuing seals, and thus they must balance the goal of ensuring responsible practices while resisting the appeal of additional revenue from companies with marginal practices.

Harvard Professor Benjamin Edelman has written one of the most comprehensive critiques of TRUSTe.²⁰⁹ In *Adverse Selection in Online "Trust" Authorities*, Edelman critiqued the incentives underlying private trust authorities, the substantive requirements of the TRUSTe system, and TRUSTe's enforcement record:

TRUSTe's postings reveal that users continue to submit hundreds of complaints each month. But of the 3,416 complaints received since January 2003, TRUSTe concluded that not a single one required any change to any member's operations, privacy statement, or privacy practices, nor did any complaint require any revocation or on-site audit.

Edelman found:

I demonstrate that sites certified by the best-known authority, TRUSTe, are more than twice as likely to be untrustworthy as uncertified sites. This difference remains statistically and economically significant when restricted to "complex" commercial sites. In contrast, competing certification system BBBOnline imposes somewhat stricter requirements and appears to provide a certification of positive, albeit limited, value.

Still, a substantial number of companies that apply for seals ultimately never obtain one, meaning that TRUSTe does identify problematic sites and deny certification. A TRUSTe certification does represent a levelling-up of practices for many sites. Defenders of seal sites argue that these self-regulator efforts will gradually improve practices, in a broad-based and sustainable fashion.

²⁰⁷ TRUSTe Watchdog Dispute Resolution and Appeal Process, available at <http://www.truste.org/consumers/compliance.php>.

²⁰⁸ TRUSTe, TRUSTe Fact Sheet, n.d., available at http://www.truste.org/about/fact_sheet.php.

²⁰⁹ Benjamin Edelman, *Adverse Selection in Online 'Trust' Certifications*, Proceedings of ICEC'09 (forthcoming) (ACM International Conference Proceeding Series), available at <http://www.benedelman.org/publications/advsel-trust.pdf>.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

The role of the FTC (2): general deference to self-regulation

The FTC has endorsed self-regulation for most of the time the agency has considered consumer privacy on the internet. The agency has been exceedingly deferential to self-regulation, and has not established metrics to determine when self-regulation would be effective or whether existing schemes have worked.

Self-regulatory initiatives taken generally subject the members' most invasive activities to opt out or no opt standards. A prime example is the IRSG's provision of opt out rights with respect to information sale to the general public. While this appeared to be a substantive right, its implementation demonstrated its illusory nature. IRSG members simply declared that their customers were not members of the "general public." LocatePlus.com implemented their obligations under IRSG with statements such as:

Companies that make nonpublic data available to the general public do offer opt outs, and, in the event that we ever make our nonpublic databases available to the general public, we will implement an opt out for individuals who request it in accordance with the IRSG principles.²¹⁰

Thus, companies subject to IRSG could comply with opt-out obligations without even administering an opt-out program.

Voluntarily-adopted standards are always substantively weaker than comparable privacy laws, and often more inconvenient to exercise than legislatively-created protections. For instance, the telemarketing do-not-call registry made irrelevant the long-established, self-regulatory DMA "telephone preference service." The DMA's self-regulatory solution made it difficult to enroll, it did not cover all telemarketers, there was no penalty for violating it, and it was difficult to find the opt out mechanism. The legislatively-created intervention, the National Do-Not-Call Telemarketing Registry, is more advantageous to consumers in every respect.

When self-regulatory groups establish opt-in protections, it usually covers activities that the groups have no commercial interest in pursuing. Or, opt-in is reserved for exceedingly narrow activities. The NAI's 2008 opt-in standard for tracking of sensitive personal information is such a narrow activity. Under this rule, NAI members voluntarily agree not to use sensitive data in "...any process used whereby data are collected across multiple web domains owned or operated by different entities to categorize likely consumer interest segments for use in advertising online."²¹¹ This narrow guarantee is further winnowed by the definition of "sensitive:" "Precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history." It is difficult to imagine a time when a network advertiser would have "precise information" about medical conditions, unless consumers began to affirmatively tell them, perhaps by sending letters stating these conditions to their mailing address.

²¹⁰ LocatePlus.com, Privacy Policy, n.d., available at <https://www.locateplus.com/privacy.asp>.

²¹¹ Network Advertising Initiative, Self-Regulatory Code of Conduct 2008 NAI Principles (2008), available at http://www.networkadvertising.org/PRIVOX-ORFORCE/networks/2008%20NAI%20Principles_final%20for%20Website.pdf.

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

Soon after the regulatory focus of the government has passed, self-regulatory groups tend to disband. For instance, the NAI constituted over 90% of the network advertising industry when it proposed guidelines in 2000.²¹² Pam Dixon found that by 2002, “just two years after the FTC recommended the NAI self-regulatory program, the NAI had only two member companies.”²¹³

The self-regulatory agreements tend to disappear from the internet too. The author, for instance, spent a significant time trying to find a copy of the 2000 NAI principles, and ultimately located it on the FTC’s website. The 2000 NAI principles do not appear on the NAI website at all, according to a Google site search of networkadvertising.org on July 23, 2009. (Ironically, the first sentence of these principles guarantees that NAI members will adhere to another self-regulatory group’s privacy policy guidelines. That other group, the “Online Privacy Alliance” appears not to have had any new news since 2001.²¹⁴)

The IRSG agreement too is elusive; it is memorialized on the website of the FTC, but does not appear at all on the website of irsg.org/.

Self-regulatory groups offer no effective enforcement remedies, and seal programs are reluctant to refer violators of privacy policies to enforcement authorities.

Finally, the nature of information technology makes self-regulatory protections vulnerable to disruptive business models. As competitors develop new business models, they are not subject to the self-regulatory schemes. And some competitors never agree to the self-regulatory limitations. For instance, while mainstream data brokers will not sell data to the “general public,” others do.

13. New Challenges

The US is taking almost no steps to prepare for the new challenges identified in this report. Generally speaking, privacy law in the US is not precautionary, but rather driven by concerns about specific public issues. For instance, video rental records enjoy very strong protections under federal and state laws, because rental records pertaining to a prominent judge and high court nominee were once released to a journalist. Until these new challenges present a public policy dilemma, they will not gain the attention of lawmakers and regulators. Furthermore, many of these challenges will occur in citizen versus state law enforcement and public safety debates, often years after the technology in question has been embraced by the government.

Increases in computing power, bandwidth and storage capacity

There is no organized public policy movement to address increases in computing power, bandwidth, and storage capacity in relation to information privacy rights. Although the Cable Communications Policy Act and the Video Privacy Protection Act both require regular deletion of consumer data, there is no general mandate for data deletion to address risks

²¹² Federal Trade Commission, *Online Profiling: A Report to Congress*, July 2000, available at <http://www.ftc.gov/os/2000/07/onlineprofiling.htm>.

²¹³ Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*, Fall 2007, available at http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

²¹⁴ See <http://www.privacyalliance.org/news/>

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

presented by greater storage. Similarly, collection limitation functions only narrowly in US law; business incentives are almost always aligned with greater collection of data.

Nanotechnology

There is no organized public policy movement to address the emerging privacy implications of nanotechnology. Existing laws may address some of the technology's misuses. For instance, existing surveillance law would prohibit the use of a nano-level device to secretly "bug" a room.

Surveillance Technologies

In *Kyllo v. United States*, the Supreme Court articulated a new standard for law enforcement adoption of advanced surveillance technologies.²¹⁵ The case involved the use of a thermal imaging device to detect heat emanating from an individual's home. Such heat may indicate the presence of a marijuana growing operation. The police used the readings from the device to obtain a warrant to search the individual's home. The Supreme Court held that the warrantless surveillance of the individual's home violated the Fourth Amendment to the US Constitution. Further when, "the government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."

Aside from *Kyllo*, there has been no successful legislative or regulatory effort to prospectively address the adoption of surveillance technologies by law enforcement. Law enforcement is an aggressive adopter of new technology, whether it be CCTV, facial recognition systems, or automated automobile license plate readers. Public policy in the US has generally tolerated this adoption. It often goes unaddressed until a defendant challenges a technology's use in the context of a criminal prosecution.

Ubiquitous Computing

Professor Deirdre K. Mulligan argues that the assumptions underlying ubiquitous computing are very different from the workings of existing US privacy law. Existing privacy law is a poor fit for technologies that collect information by default, that do so silently, and can develop new patterns from putatively unrelated data.²¹⁶ A large research effort surrounds incorporating privacy design principles into ubiquitous computing,²¹⁷ but no US sectoral law or legislative effort addresses the privacy risks of the technology.

Biometrics

The US has aggressively expanded biometrics programs after the September 11, 2001 terrorist attacks. Some existing US privacy laws apply to biometric information, depending upon the context in which they are captured. For instance, the Privacy Act protects citizens' records in control of federal agencies.

²¹⁵ 533 U.S. 27 (2001).

²¹⁶ Deirdre K. Mulligan, *Privacy and Sensor Networks: Do Sensor Networks fit with. Fair Information Practices*, available at <http://www.eecs.berkeley.edu/~culler/citris/sensorday/mulligan.ppt> .

²¹⁷ See e.g. <http://www.truststc.org/pubs/search/?groupname=sensornets&Action=Search> .

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

However, there is no organized, forward looking regulation to address expanding collection of biometrics, or the expanding array of technologies that purport to reliably identify individuals.

As with many other emerging privacy issues, state legislatures may be the first to address the implications of biometrics technology. The recently enacted Illinois Biometric Information Privacy Act creates consent requirements before the private sector collects biometrics from individuals, requires the creation of security policies, and requires destruction of the biometric identifier if the individual does not interact with the business for three years.²¹⁸

Identity Management

The US has not created a formal national identification system. Nor has it created an identity infrastructure similar to countries with national identification systems. Many Americans do not possess a passport, and thus their most authoritative identity document is a state-issued identity card or drivers license. Political and technical concerns²¹⁹ make the issue highly charged.

The 2005 “REAL ID” Act set forth minimum requirements for state issuance of driver licenses. Under the Act’s approach, states would have to comply with these standards, otherwise drivers licenses could not be used to gain entrance to federal facilities (including airports).

In August 2004, President Bush issued Homeland Security Presidential Directive 12, which calls for a common identification standard for federal employees and contractors. The government has created a website to foster discussion of citizen, business, and employee authentication.²²⁰

The most forward-looking work on identity management is occurring in the private sector. The OpenID Foundation, the Info Card Foundation, and InCommon Federation are examples of identification initiatives.

Data mining and profiling

A nascent political movement calls for updating the Privacy Act, because its protections, even after data matching amendments, have fallen short in addressing data mining and profiling by the government.²²¹ The Privacy Act was developed in an era of mainframe computers, and changes in technology, culture, and the political landscape render it ineffective to address new challenges in data mining and profiling.

²¹⁸ Public Act 95-0994, available at <http://www.ilga.gov/legislation/95/SB/PDF/09500SB2400enr.pdf> .

²¹⁹ National Academies of Sciences, IDs -- Not That Easy: Questions About Nationwide Identity Systems (2002) Computer Science and Telecommunications Board (Stephen T. Kent and Lynette I. Millett, Editors), available at <http://www.nap.edu/openbook.php?isbn=030908430X> .

²²⁰ <http://www.idmanagement.gov/> .

²²¹ See e.g., Information Security and Privacy Advisory Board, Toward a 21st Century Framework for Federal Government Privacy Policy (May 2009), available at <http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-report-may2009.pdf> ;

E-Commerce and advertising

The US approach to e-commerce and advertising has been reactive. As explained above, a series of Federal Trade Commission and Attorneys General actions have shaped the rules of how e-commerce companies and advertising companies use data. For much of the FTC's time in shaping online privacy, it has followed a notice and consent paradigm, and prioritized protections for shielding consumers from harm. This approach may be changing. In a recent case, the FTC settled an action with a company that tracked users' online browsing.²²² The company notified the users of the tracking in an end user license agreement, and even paid each user \$10 for downloading a program that enabled the tracking. Nevertheless, the FTC determined that the company violated the Federal Trade Commission Act because it did not adequately inform users of the scope of the software's data collection. This may mark a departure from a strict notice and choice approach; it may indicate that there are some practices that pro forma notices cannot justify, and in practical application, it may be impossible to give adequate notice of some practices. If this avenue of reasoning is followed, online privacy regulation may start to resemble US consumer law in other contexts, where many business practices are illegal even if they occur with notice and consent.

A recent enforcement action by the New York Attorney General is worthy of note here. In the Datan Media case, the New York Attorney General pursued a marketing company for buying a list of personal information from websites that promised not to sell data.²²³ One data supplier had assured consumers on several web sites it owned and operated that it would "never lend, sell or give out for any reason" the information provided by users. The Attorney General's investigation determined that Datan knew of a promise to consumers when it purchased the consumer lists. But after obtaining these lists, Datan sent millions of unsolicited e-mails to the listed consumers.

This theory of liability has not been pursued by other attorneys general or the Federal Trade Commission. However, it offers great promise in better ensuring that companies trading in data understand the provenance of personal information, and the restrictions and expectations set by users.

Social networking and user generated content

There is no public policy movement (aside from consumer education) to address the phenomenon of self-revelation of data on social network sites. This has gone unaddressed, despite that self-revelation seems to be a goal of the companies operating these sites,²²⁴ and despite the fact that employers can use internet searches and social networking service information to screen job applicants without implicating the Fair Credit Reporting Act. Social networking services have also become a trove for law enforcement investigations.

²²² In re Sears Holdings Management Corp., FTC, No. 082 3099, available at <http://www.ftc.gov/os/caselist/0823099/index.shtm>.

²²³ Kevin Newcomb, E-mail Marketer Slapped for Privacy Violations, ClickZ, Mar. 13, 2006, available at <http://www.clickz.com/3591116>.

²²⁴ Michael Zimmer, Facebook's Zuckerberg on Increasing the Streams of Personal Information Online, Nov. 8, 2008, available at <http://michaelzimmer.org/2008/11/08/facebooks-zuckerberg-on-increasing-the-streams-of-personal-information-online/>.

E-government and public administration

The E-Government Act of 2002²²⁵ represented a notable improvement in the practice of public administration in the US. That Act required federal agencies to create privacy impact assessments (PIA) before developing or procuring information technology or initiating any new collections of personally-identifiable information.²²⁶ These requirements were heralded for their ability to motivate more adoption of PETs and to increase the privacy sensitivity of agency decision making.

Health and social care systems

The US is involved in a heated debate about the future of health and social care systems. Federal government health care programs are subject to Privacy Act protections. But without universal health care, many Americans go uninsured, seek private insurance, or are insured through their employer. The Privacy Rule promulgated as a result of the Health Insurance Portability and Accountability Act regulates these interactions, as does principles of employment law when insurance is provided through an employer.

Law enforcement and intelligence

The US is not proactively addressing new challenges raised by law enforcement and intelligence activities. Under the US approach, law enforcement and intelligence agencies can adopt new technologies and techniques without Congressional or Judicial oversight (unless these technologies and techniques implicating existing privacy laws). Thus, new biometrics systems, video surveillance, and other systems have been adopted without precautionary oversight.

Even where intelligence agencies engage in problematic activities implicating existing privacy laws, the US government has blocked oversight and accountability measures. For instance, after it was revealed that the National Security Agency had access to vast amounts of telecommunications data, the US Congress enacted laws to interfere with suits brought against the telecommunications companies.²²⁷

Globalisation and the Internet

The US has not passed a sectoral law to address globalization and increased use of the Internet. The country is guided by self-regulatory norms, and enforcement actions by the Federal Trade Commission. US internet companies are covered by sectoral laws based upon their area of operation, just like offline companies. Thus the incoherent, uneven landscape is still present: an online video rental company would be subject to the Video Privacy Protection Act, while an online seller of the same videos would not be covered by any sectoral law.

²²⁵ Pub. L. 107-347.

²²⁶ For an in-depth review of administrative agency decisionmaking in the PIA context, see Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy Decisionmaking in Administrative Agencies, 75 University of Chicago Law Review 75 (2008)(analysis points to the “importance of internal agency structure, culture, personnel, and professional expertise as important mechanisms for ensuring bureaucratic accountability to the secondary privacy mandate imposed by Congress.”)

²²⁷ FISA Amendments Act of 2008, P.L. 110-261, available at <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:H.R.6304>:

Privacy enhancing technologies and privacy by design

There is a very strong research movement in the US surrounding privacy enhancing technologies and privacy by design. The problem comes in incentives: there is little reason to adopt these technologies except where a business experiences direct costs from the collection of personal information. Thus, much thought and action has been concentrated on incorporating privacy technologies and design into businesses that are subject to security breach notification laws. Outside those contexts, generally, incentives are aligned with information collection rather than privacy by design.

III. Summary and conclusions

The USA follows a sectoral model for privacy protection. This gives businesses the opportunity to develop new products and services that fall within the gaps of privacy protection left by the sectoral model. It also results in an incoherent, uneven landscape of protection for data.

Summary of data protection in the USA

Several approaches in the US system are worth noting, for the efficacy in changing institutional practices dramatically. These interventions are incentives-based, and less likely to involve prescriptive mandates for personal information.

First, performance-based standards can foster “compliance plus.” In the information security context, security breach notification laws avoided prescriptive rules for securing information, leaving government and companies responsible for figuring out the “how” of information security. This approach only punishes them for failure.

One could imagine regimes that largely leave the responsibility for determining how to protect privacy to data collectors, with carrots and sticks accruing to the entity based upon certain performance standards. Such an approach could move data collectors out of a compliance mindset, into one that is results oriented. This approach has the potential to reduce the problem of reification in practices from prescriptive mandates.

Second, advertiser liability can be an effective tool for addressing direct marketing that contravenes privacy law. As direct marketing service providers use innovative techniques to mask their identity and practices, holding the advertiser that hired them liable creates due diligence and supervision incentives thereby curbing abuses.

Third, auditing of access has changed the landscape of several sectors. Most notably, auditing in health care has documented and substantiated the long-suspected practice of medical file “browsing.” New technologies, such as email or SMS alerts, could be leveraged to inform individuals of access to their files, and thus enable self-policing of browsing and identity theft problems.

Fourth, data provenance is an underexamined approach that could create strong incentives for accountability in the data trade. Section 10.8 above mentions the Datan Media case, where a purchaser of information was held liable because the seller violated promises to the data subjects concerning non-disclosure. This theory of liability has not been further pursued by

EUROPEAN COMMISSION – DG JFS
NEW CHALLENGES TO DATA PROTECTION
Country Study B.1 – United States of America

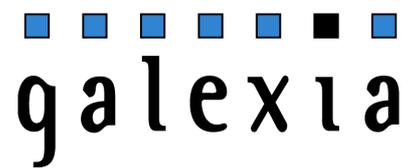
US authorities. But just as third-party advertiser liability can create incentives to police direct marketing abuses, “data provenance” responsibilities can create incentives to reduce gray and black market sales of personal information.

Finally, the US approach allows states to enact stronger protections where the federal government has not taken action, and even where the US Congress has created privacy rules, states are typically allowed to enhance them. This dual-level approach has allowed fast-acting states to identify and attempt to remedy emerging privacy problems. Indeed, many federal-level privacy protections were originally products of state legislatures (e.g., security breach notification, rights for victims of identity theft). Allowing state experimentation allows a superior authority to weigh different approaches, and to codify ones effective in remedying a privacy problem.

Position in relation to international standards

In many respects, the US is a data haven in comparison to international standards. Increasing globalization of US business, evidenced by the Safe Harbor agreement, is driving more thinking about data protection in other countries. Still, political and economic forces make a European-style data protection law of general applicability highly unlikely in the near future.

- o – O – o -



The US Safe Harbor - Fact or Fiction? (2008)

Chris Connolly, Galexia¹



¹ Chris Connolly is a Director of Galexia, an independent consultancy specialising in privacy and electronic commerce.
<<http://www.galexia.com.au>>.

Document Control

Version

1.0

Date

2 December 2008

Source

The latest version of this article is available from

http://www.galexia.com/public/research/articles/research_articles-pa07.html

Copyright

Copyright © 2008 Galexia.

Contents

1.	Introduction	4
2.	Previous reviews of the Safe Harbor Framework.....	5
3.	Safe Harbor participants	6
4.	Compliant members	7
5.	Detailed Findings	8
	5.1. <i>False claims regarding membership</i>	8
	5.2. <i>False claims regarding certification</i>	9
	5.3. <i>The Safe Harbor Certification Mark</i>	10
	5.4. <i>Availability of privacy policies</i>	11
	5.5. <i>Content of privacy policies</i>	12
	5.6. <i>Participation in privacy programs</i>	12
	5.7. <i>Dispute resolution providers</i>	13
	5.8. <i>Co-operation with the EU DPA Panel</i>	15
	5.9. <i>Categories of data protected</i>	16
6.	Recommendations.....	16
	6.1. <i>Recommendations for the EU</i>	16
	6.2. <i>Recommendations for the US</i>	17
7.	Appendix – Methodology for this study.....	18

1. Introduction

The US Safe Harbor is an agreement between the European Commission and the United States Department of Commerce that enables organisations to join a Safe Harbor List to demonstrate their compliance with the European Union Data Protection Directive. This allows the transfer of personal data to the US in circumstances where the transfer would otherwise not meet the European adequacy test for privacy protection.

The first public draft of the Safe Harbor Principles was released in November 1998², although they were not officially accepted by the EU until 2000.

The Safe Harbor is best described as an uneasy compromise between the comprehensive legislative approach adopted by European nations and the self-regulatory approach preferred by the US. The Safe Harbor Framework has been the subject of ongoing criticism, including two previous reviews (2002 and 2004). Those reviews expressed serious concerns about the effectiveness of the Safe Harbor as a privacy protection mechanism.

After ten years of public debate it is time to examine the Safe Harbor again. This article summarises the findings of a Galexia study regarding the current status of the Safe Harbor Framework. The Galexia study assessed each of the organisations listed on the Safe Harbor List (1,597 entries) against a small subset of key criteria contained in the Safe Harbor Framework Principles.

This study raises concerns that many aspects of the Safe Harbor Framework are not working. Highlights of this study include:

Compliance:

- Although the list contained 1,597 entries, only 1,109 organisations were current members of the Safe Harbor Framework. Many organisations on the list no longer exist or they have failed to renew their certification. The list also includes double entries.
- Only 348 organisations meet even the most basic requirements of the Safe Harbor Framework. Many organisations did not have a public privacy policy, or the policy failed to even mention the Safe Harbor. A large number of organisations failed to comply with Principle 7 – Enforcement and Dispute Resolution, as they did not identify an independent dispute resolution process for consumers.
- 209 organisations selected a dispute resolution provider that was not affordable. These include the American Arbitration Association (AAA) that costs between \$120 and \$1,200 per hour (with a four-hour minimum charge plus a \$950 administration fee), and the Judicial Arbitration Mediation Service (JAMS) that costs \$350 to \$800 per hour (plus a \$275 administration fee). Organisations either failed to disclose these costs or required the consumer to share these costs.

False and/or misleading information:

- 206 organisations claim on their public websites to be members of the Safe Harbor when they are not current members. Many of these false claims have continued for several years.

² <<http://www.ita.doc.gov/td/ecom/aaron114.html#Safe>>

- 36 of these 206 false claimants were also accredited by a third party as being current members of their Safe Harbor trustmark scheme (e.g. the TRUSTe Safe Harbor and BBB Safe Harbor programs), even though these organisations are not current members of the official Safe Harbor.
- 73 organisations claimed to be members of a Privacy Trustmark Scheme (e.g. TRUSTe or the BBB Safe Harbor program) when they are not current members of those schemes, or they claimed to be members of BBB Online Privacy – a scheme that closed 18 months ago and has not accepted any complaints since June.
- 20 organisations displayed a Department of Commerce Safe Harbor ‘seal’ on their website when they were not actually compliant with the Safe Harbor Framework, including numerous unauthorised seals created using graphics software.
- 24 organisations claimed that they had been certified by the Department of Commerce or certified by the EU – when the Framework is actually based on self-certification.

Overall the study found numerous problems with data accuracy and basic compliance with simple Framework requirements. This study only checked for compliance with one of the seven Safe Harbor Framework Principles (Principle 7 – Enforcement and Dispute Resolution). Galexia did not check the other six principles. Only 348 organisations passed this basic test of compliance with Principle 7.

It is unlikely that many of these 348 organisations would be considered compliant with the more detailed requirements of the other six Safe Harbor Framework Principles. For example, some organisations’ privacy policies are only two sentences long.

Overall the study found that the problems identified in previous reviews of the Safe Harbor have not been rectified, and that the number of false claims made by organisations represents a significant privacy risk to consumers.

The Galexia study is part of a broader comparative study of privacy legislation and privacy self-regulation.³

2. Previous reviews of the Safe Harbor Framework

It is important to note that the manager of the Safe Harbor Framework – the US Department of Commerce – holds the Safe Harbor Framework in very high regard, and considers it a success. In October 2007 the Department of Commerce claimed that the ‘EU view Safe Harbor as a Best Practice and Gold Standard for data protection’.⁴

There is, however, no other evidence available that the EU view the Safe Harbor as a ‘gold standard’ – the more common view is that the Safe Harbor is a practical compromise. The EU reviewed the Safe Harbor in 2002 and again in 2004. Both studies raised significant concerns.

³ See also: Connolly C, *Trustmark Schemes Struggle to Protect Privacy*, 26 September 2008, <http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/> and Connolly C, *Asia-Pacific Region at the Privacy Crossroads*, 25 August 2008, World Data Protection Report, volume 8, number 9, <http://www.galexia.com/public/research/assets/asia_at_privacy_crossroads_20080825/>.

⁴ Greer D, *The U.S.-E.U. Safe Harbor Framework*, presentation to the Conference on Cross-Border Data Flows, Data Protection, and Privacy, Washington DC, October 2007, <http://www.SafeHarbor.govtools.us/documents/1A_DOC_Greer.ppt>.

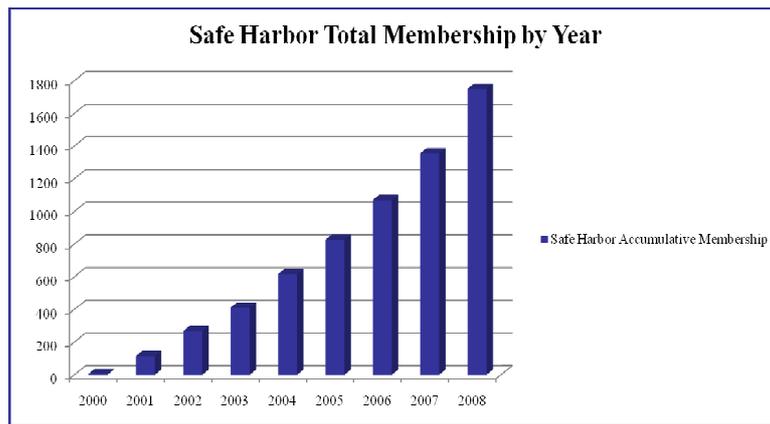
The 2002 review found that ‘a substantial number of organisations that have self-certified adherence to the Safe Harbor do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies. Transparency is a vital feature in self-regulatory systems and it is necessary that organisations improve their practices in this regard.’ The 2002 review was also critical of the available dispute resolution mechanisms at that time.⁵

The 2004 review examined 10% of Safe Harbor organisations in detail, resulting in a long list of criticisms, including concerns that a number of companies failed to identify an Alternative Dispute Resolution body. They also raised concerns that ‘some alternative recourse mechanisms still fail to comply with applicable Safe Harbor requirements’ and ‘less than half of organisations post privacy policies that reflect all seven Safe Harbor Principles’.⁶

3. Safe Harbor participants

In October 2008 the Department of Commerce claimed that ‘today, nearly 1,700 U.S. organizations [have] certified to Safe Harbor’.⁷ The public website for the Safe Harbor states that ‘more than 1,500 U.S. companies participate in the Safe Harbor’.⁸

The Department of Commerce also publish the following chart⁹ to display total membership:



⁵ European Commission, *The application of Commission Decision on the adequate protection of personal data provided by the Safe Harbor Privacy Principles*, 13 February 2002, page 2, http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf.

⁶ European Commission, *The implementation of Commission Decision on the adequate protection of personal data provided by the Safe Harbor Privacy Principles*, 20 October 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf.

⁷ Greer D, *The U.S.-E.U. Safe Harbor Framework - Past, Present, & Future*, presentation to the Workshop On International Transfers Of Personal Data, Brussels, 21 October 2008, http://ec.europa.eu/justice_home/news/information_dossiers/personal_data_workshop/doc/Presentation_Greer.ppt.

⁸ http://www.export.gov/SafeHarbor/Safe_Harbor_Announcement.asp

⁹ Greer D, *The U.S.-E.U. Safe Harbor Framework - Past, Present, & Future*, presentation to the Workshop On International Transfers Of Personal Data, Brussels, 21 October 2008, http://ec.europa.eu/justice_home/news/information_dossiers/personal_data_workshop/doc/Presentation_Greer.ppt.

Although the graph carries the label ‘accumulative membership’, this is not correct. Galexia downloaded the Safe Harbor list on 17 Oct 2008 and there were 1,597 records (including 19 doubles, triples and the test file).¹⁰ However, 342 of these organisations were listed as ‘not current’ by the Department of Commerce. A further 136 organisations have failed to renew their certification by the required date and are listed as ‘not current’ in this study, bringing the total of ‘not current’ organisations to 478.

Allowing a generous 6 week grace period for renewals only reduces the number of ‘not current’ organisations by 18. This is because the vast majority of ‘not current’ organisations have ceased to exist, have left the Safe Harbor permanently, or have failed to renew for 6 months or longer.

Claims that the cumulative membership of the Safe Harbor are approaching 1700, or that 1500 companies ‘participate’ in the Safe Harbor are simply incorrect. Once doubles, triples and ‘not current’ organisations are removed, only 1109 organisations remain.

4. Compliant members

The study found that only 348 organisations meet even the most basic requirements of the Safe Harbor Framework. This figure was reached using the following steps:

Membership Requirement	Notes	Number of entries	Number of unique entries removed	Cumulative total
Organisation is listed.	All organisations listed on 17 October 2008.	1597	0	1597
Unique entry	Removes doubles, triples and the test file	19	19	1578
Collects EU personal information	Removes irrelevant organisations who do not collect any EU personal information	7	7	1571
Listed as current by DOC	Removes organisations listed by the Department of Commerce as ‘not current’	342	329	1242
Listed as current by certification renewal date	Removes organisations that failed to renew by 17 October 2008.	477	133	1109
Website privacy policy is accessible	Removes organisations who claim to have a website privacy policy, but it is unreachable.	175	57	1052
Privacy policy mentions Safe Harbor	Removes organisations who have a public privacy policy but it does not mention the Safe Harbor at all	218	127	925
Privacy policy complies with the enforcement principle	Removes organisations who have a public privacy policy that does not provide information on the selected dispute resolution provider.	587	279	646
Affordable dispute resolution provider.	Removes organisations who have selected AAA or JAMS as their dispute resolution provider in either their certification record or their public privacy policy.	209	107	539
Verified member of TRUSTe dispute resolution.	Removes organisations who have selected TRUSTe as their dispute resolution provider when they are not current members.	29	11	528
Verified member of TRUSTe privacy program	Removes organisations who claim to be members of the TRUSTe privacy program when they are not current members	30	2	526

¹⁰ On 17 November 2008 there were 1633 records.

Membership Requirement	Notes	Number of entries	Number of unique entries removed	Cumulative total
Verified member of the BBB Safe Harbor program	Removes organisations who claim to be members of the BBB Safe Harbor program when they are not current members.	4	3	523
Dispute resolution provider exists	Removes organisations who have selected BBB Online Privacy as their dispute resolution provider (closed in July 2008)	21	15	508
Privacy program exists	Removes organisations who claim to be members of BBB Online Privacy (closed in July 2008)	31	3	505
No website privacy policy	Removes organisations who require a password or direct contact in order to obtain their privacy policy.	246	151	354
No misleading information	Removes organisations who are using unauthorised Safe Harbor seals or who claim they have been certified by the Department of Commerce or the EU	32	6	348

The 348 organisations that are listed as compliant with these basic Safe Harbor requirements, may not in fact be compliant with all seven of the more detailed Safe Harbor Principles, as this study only assessed compliance with Principle 7.

It is also important to note that although an organisation may be listed here as compliant, it may have restricted the scope of its Safe Harbor membership to a particular category of data. For example 41 of these organisations have restricted the scope of their Safe Harbor membership to human resources data only.

Of the 348 organisations who were found to be compliant in this study, only 54 extended their Safe Harbor membership to all data. This is extremely important. Out of the 1,597 entries on the Safe Harbor list only 54 are compliant with basic Safe Harbor requirements for all categories of data – only 3% of organisations on the list.

5. Detailed Findings

5.1. False claims regarding membership

206 organisations claim to be members of the Safe Harbor when they are not current members. The oldest false claim dates back to June 2003 (i.e. the last date they were actually a member of the Safe Harbor). More than half (112) of the false claims are over twelve months old.¹¹ There is a significant risk that EU consumers and businesses will be misled by these claims.

Unfortunately, membership of a third party privacy program does not necessarily lower the incidence of false claims. 26 organisations certified as TRUSTe EU Safe Harbor members are not actually on the current Safe Harbor list. The oldest of these false claims dates back to September 2005, and 11 of these false claims are more than one year old.

¹¹ Galexia has captured and date-stamped screenshots or files for these 206 false claims.

In most jurisdictions an organisation would face serious consequences for making a false claim of this nature, and even a single breach by a single company would result in regulatory action. In the US there is no indication that this issue has been the subject of any action by authorities, despite the hundreds of false claims over a lengthy period.

5.2. False claims regarding certification

The Safe Harbor is a self-certification scheme, and most organisations reflect this in the text of their privacy policies. However, great care needs to be taken regarding claims that US organisations have been ‘certified by the Department of Commerce’ or even ‘certified by the EU’. There are also some references to the ‘Safe Harbor Act’ that may mislead consumers, as the Safe Harbor is not a legislative regime.

This study identified a large number of organisation making false claims, using the following words (or similar):

Claim	Location
In the case of the USA, the Safe Harbor Act protects EU citizens and allows transfer of personal data so long as the recipient (Company X) is a certified signatory to the Act.	Company privacy policy
Company X Awarded EU Safe Harbor Certification to Become the First Certified U.S.-based Email Provider.	Company blog
Collection and transfer of this data between Company X Worldwide and its regional offices and/or member firms is allowed through explicit consent as a member and through adherence of Company X Worldwide regional offices to the Safe Harbor Act in Europe.	Company privacy policy
Company X announced today that it has been certified by the U.S. Department of Commerce as compliant with the United States-European Union (EU) Safe Harbor Framework.	Company press release
Company X is certified by the Department of Commerce. We have implemented the Safe Harbor principles and comply with all Safe Harbor principles. Visit http://www.export.gov/SafeHarbor and chose Safe Harbor list to review our certification.	Company privacy policy
Company X today announced that it has received Safe Harbor Certification from the U.S. Department of Commerce... 'Receiving our Safe Harbor Certification from the Commerce Department will enhance our capabilities to better serve our European clients'.	Company press release
Company X Joins European Privacy Safe Harbor - Under Safe Harbor, US companies are certified by the EU as providing acceptable privacy protection as defined by the European Commission.	Company press release
We have obtained certification of our compliance with the U.S. Department of Commerce's Safe Harbor program for United States businesses – the so-called EU Safe Harbor.	Company privacy policy
Company X Receives Safe Harbor Certification - US Department of Commerce Certifies Company X 's Data Security - Company X has formalized and documented its data privacy procedures and obtained Safe Harbor Certification from the U.S. Department of Commerce.	Company press release
This Policy is registered and certified with the U.S. Department of Commerce Safe Harbor program.	Company privacy policy
Company X joins a distinguished group of global firms that have met the strict European standard for data privacy protection. The U.S. Department of Commerce and the European Safe Harbor Commission have recently awarded Company X its Safe Harbor certification	Company press release

5.3. The Safe Harbor Certification Mark

The Department of Commerce recently issued a ‘Safe Harbor Certification Mark’ that can be used by organisations as a ‘visual manifestation of the commitment your organization makes when it self-certifies that it will comply with the U.S.-EU Safe Harbor Framework’.¹²



This is a dangerous development and is already resulting in misleading information for consumers. 26 organisations currently display the Certification Mark, but only 13 of these organisations are compliant with the basic Safe Harbor requirements.

The Certification Mark may imply that the site has been endorsed by the Department of Commerce, when the Safe Harbor is merely a self-certification scheme. The Certification Mark is supposed to be preceded by the words ‘we self-certify compliance with’, although these words do not appear in the graphic itself. One organisation is already using the graphic without the ‘self certify’ words.

The Certification Mark implies that all information provided to the site will be protected by the Safe Harbor. There is only one logo – rather than separate logos for human resources data, online data, offline data etc. Most organisations restrict the scope of their Safe Harbor membership to 1-2 categories of data.

There is also widespread evidence that organisations have simply made up their own Safe Harbor seals and added them to websites, surveys, emails etc. Consider the following examples:

Organisation	Notes	Logo
Surveygizmo	This site states: ‘At the request of customers, here are graphic ‘badges’ you can place in your survey, email or web page to showcase your compliance.’ They are not actually members of the Safe Harbor.	
Delphi Corporation	Their Safe Harbor Policy contains a large Department of Commerce logo without explanation.	
Background Profiles	Their Privacy Notice has an unauthorised Department of Commerce Safe Harbor logo.	
Mind Your Business Inc	This unauthorised Department of Commerce logo is prominently displayed on their home page.	
Acton Inc	This unauthorised Department of Commerce logo appears on their home page next to the words ‘Safe Harbor’.	

¹² <http://www.export.gov/SafeHarbor/Safe_Harbor_Instructions.asp>

Organisation	Notes	Logo
Saturn Inc	This Department of Commerce logo appears on their Privacy Policy next to the word 'Associations'. Their entire privacy policy is two lines long.	

In most jurisdictions there are serious repercussions if a company uses a Government coat of arms or logo on their website in a way that implies Government endorsement of the company. There is no indication of such concern in the United States and the Galexia study found that there are actually more unauthorised / misleading seals in use than there are authorised / accurate seals.

5.4. Availability of privacy policies

The entire legal basis of the Safe Harbor relies on a privacy policy being available, so that a comparison can be made between privacy promises and privacy practices. If there is a difference between the promise and the practice, the Federal Trade Commission will have jurisdiction to act using their general consumer protection powers. If no privacy policy is available, the organisations will not be compliant with the US Safe Harbor and there may be no legal basis for enforcement action:

The FTC has powers to pursue companies which make false or misleading statements in their privacy policies, but it is doubtful whether it would have jurisdiction over those that fail to actually publish the required statements. In those cases ... it would be very hard for any kind of enforcement action to proceed in the United States.¹³

The 2004 EU review of the Safe Harbor stressed the importance of privacy policies being available for public review:

Lack of a public self-statement in itself means that Safe Harbor participants are falling short of what the decision requires. To comply with the Safe Harbor, a company must be subject to enforcement actions by the FTC. The FTC's authority to enforce the Principles upon a given organisation is triggered by such an organisation's public commitment to comply with the Principles. Without such a public commitment, the FTC would not have the authority to enforce the Principles. This basically puts the company that lacks a publicly available privacy policy that fully embraces the Principles in non-compliance.¹⁴

The Galexia study found that many organisations do not make their privacy policies available. The following table summarises the availability of privacy policies:

Availability	Number of Organisations
Not Available – Contact Required Requires contact with the organisation, often an email address is supplied or the location requires a password.	246

¹³ Pedersen A, *US Safe Harbor under fire*, Privacy Law and Business Reporter, issue 75, October 2004, page 10, <http://www.hunton.com/files/tbl_s47Details/FileUpload265/912/Safe_Harbor_Sotto_11.04.pdf>.

¹⁴ EU 2004 review, page 6.

Availability	Number of Organisations
Not Available – Absent The website does not have a privacy policy or access to the privacy policy is permanently broken. In this study access was attempted using both Internet Explorer and Mozilla Firefox. Searches included home pages, contact sections, 'about us', FAQs etc.	175
Available – Findable using search The Department of Commerce self-certification entry was incorrect, but the privacy policy could be found using simple site searches.	208
Available – Accurate link provided Accurately linked or clearly on the home page (includes correcting basic typos).	966

5.5. Content of privacy policies

The quality of the content of privacy policies varies significantly. Major issues identified in this study include:

- Numerous privacy policies are only 1-3 sentences long and contain virtually no information for consumers. The shortest EU Safe Harbor privacy policy simply stated: 'Company X maintains privacy measures that exceed Safe Harbor requirements'.
- Numerous privacy policies simply refer the consumer to the Department of Commerce Safe Harbor website for further details.
- Numerous privacy policies appear to conform to a common 'template' privacy policy that is not compliant with the Safe Harbor Framework. This template has a heading called 'enforcement' or 'dispute resolution' and then has text telling the consumer that if their complaint cannot be resolved with the organisation, they should 'contact your local Data Protection Authority for further information'. There is no other information on independent dispute resolution, and no discussion of the Panel. This template accounts for a significant number of non-compliant sites.
- Numerous privacy policies claim that the organisation is compliant with the Safe Harbor without providing any explanation about what the Safe Harbor is. One example just says 'Customers from the European Union should note that we are in compliance with the Safe Harbor privacy principles.' No further details are provided.

5.6. Participation in privacy programs

The self-certification form asks organisations to 'List any privacy programs in which your organization is a member for Safe Harbor purposes'. This is followed by a box where free text can be entered.

The exact purpose of this part of the self-certification is not clear. There is no requirement to join a privacy program. However, if text is entered here then it is important that the information is accurate. Care needs to be taken not to raise expectations that the 'privacy programs' play any formal role in the Safe Harbor arrangements (there is another box later in the form covering dispute resolution providers – who do play a formal role in the Safe Harbor).

Common entries in this section are TRUSTe (176), BBB (93) and DMA (67).

A range of additional organisations are listed as ‘privacy programs in which your organization is a member for Safe Harbor purposes’. However, none of these appear to be programs that cover privacy issues relevant to the Safe Harbor. Some entries are irrelevant or difficult to explain. Many entries appear to confuse privacy compliance with security compliance – and these entries generally indicate a lack of understanding about the Safe Harbor program. Entries include:

Privacy Program	Comments
American Arbitration Association	No relevant privacy program
American Society for Industrial Security (ASIS)	No relevant privacy program
Center for Internet Security	No relevant privacy program
Comodo	Comodo is a firewall provider
European Privacy Officers Network	No relevant privacy program
Gramm-Leach-Bliley Act (GLBA)	GLBA is federal legislation
HIPAA	HIPAA is federal legislation
International Association of Privacy Professionals	No relevant privacy program
International Security Forum	No relevant privacy program
ISO 9001	Not relevant
Privacy Alliance	Inactive
Statement on Auditing Standards No. 70: Service Organizations (SAS 70)	Not relevant
Tulsa Metro Chamber of Commerce	No relevant privacy program.
US Council for International Business (USCIB)	No relevant privacy program
Equifax	?

5.7. Dispute resolution providers

One of the most important compliance requirements in the Safe Harbor is Principle 7 – Enforcement and Dispute Resolution. This requires organisations to select an independent dispute resolution provider – usually indicated in the self-certification entry and/or the public privacy policy.

Compliance with this requirement is confusing, as many organisations select multiple dispute resolution providers or indicate the ‘brand’ of dispute resolution (e.g. BBB) without clearly indicating which specific BBB program they have selected. There is also enormous inconsistency between the dispute resolution provider selected in the self-certification form, and the provider mentioned in the website privacy policy.

The following table is therefore a very rough summary of the dispute resolution providers selected by organisations:

Dispute Resolution Provider	Number of Organisations	Compliance	Notes
Entry is blank	9	Non compliant	
Entry provides an email address only	2	Non compliant	
AAA	184	Non compliant	The American Arbitration Association (AAA) costs between \$120 and \$1,200 per hour (with a four-hour minimum charge plus a \$950 administration fee).

Dispute Resolution Provider	Number of Organisations	Compliance	Notes
BBB	106	Confusing	The BBB Safe Harbor program is compliant, but it is often unclear whether an organisation is indicating that it is a member of another BBB program (eg the Reliability program), a former BBB program (e.g. the closed Online Privacy program), or whether they just mean a consumer can take their complaint to a generic BBB office.
BBB EU	37	Compliant	This number is likely to be higher as some organisations that have stated 'BBB' will actually belong to the BBB EU program.
BBB Online Privacy	32	Not compliant	This program is closed. This number is likely to be slightly higher as many organisations that have stated 'BBB' will actually belong to the BBB Online Privacy program.
DMA	112	Compliant	
EU DPA Panel	870	Compliant	
JAMS	25	Non compliant	The Judicial Arbitration Mediation Service (JAMS) costs \$350 to \$800 per hour (plus a \$275 administration fee).
TRUSTe (generic)	61	Confusing	The generic TRUSTe program cannot receive complaints regarding offline data, and may therefore not be suitable in all circumstances. This number is likely to be lower as some organisations have only entered 'TRUSTe' on the form without indicating the specific TRUSTe scheme they belong to.
TRUSTe Safe Harbor	110	Compliant	This number is likely to be higher as some organisations have only entered 'TRUSTe' on the form without indicating the specific TRUSTe scheme they belong to.

The key requirements for dispute resolution providers are that they are independent, affordable and they can provide an appropriate range of sanctions.

This study did not include a detailed examination of the independence of the selected dispute resolution providers. However a problem regarding independence was noted in passing. Nearly all members of the TRUSTe program state in their privacy policies that 'TRUSTe is a worldwide, independent, non-profit organization'. This common wording is in fact incorrect and misleading. TRUSTe abandoned its non-profit status in July 2008 and is now a for-profit company. Its major shareholders are venture capital firm Accel – also substantial investors in Facebook. References to TRUSTe being non-profit should be removed immediately. Even the Facebook privacy policy states that TRUSTe is an 'independent, non-profit organization' – many months after the change in status.

Affordability is also a major issue. The Safe Harbor FAQ 11: states that 'the recourse available to individuals must be readily available and affordable'. In all European jurisdictions access to an independent dispute resolution service regarding privacy is free.

Two key Safe Harbor dispute resolution services (selected by 209 Safe Harbor members) are too expensive for ordinary consumers to utilise:

- **The American Arbitration Association (AAA)**
 An arbitrator with the AAA charges between \$120 and \$1,200 per hour (with a four-hour minimum charge). There is also a minimum \$925 administration fee for international disputes, that rises depending on the amount of money in dispute. Many privacy complaints will not include a claim for money – in these cases AAA charges a \$4,500 administration fee for 'non-monetary amounts'.¹⁵ These fees do not include additional costs such as the hire of a hearing room or telephone conference.

¹⁵ <<http://www.adr.org/si.asp?id=5385>>

- **The Judicial Arbitration Mediation Service (JAMS)**
 JAMS costs \$350 to \$800 per hour (plus a \$275 administration fee). It is also a significant challenge to find detailed fee information regarding JAMS – there is virtually no disclosure of detailed costs on the JAMS website and their panel of neutrals do not publish a fee schedule.

No Safe Harbor member in this study revealed the extent of these costs to consumers in their privacy policy. Some organisations include a clause in their privacy policy requiring the consumer to share these costs.

5.8. Co-operation with the EU DPA Panel

The Safe Harbor enforcement principle requires organisations to identify an independent dispute resolution provider. However, it allows organisations to select an alternative approach – they may agree to cooperate with the dispute resolution Panel established by the EU Data Protection Authorities. Indeed, this approach is required for all human resources data.

Evidence of this ‘agreement to cooperate’ is essential, as the 2002 and 2004 EU reviews both found that it was necessary for a US organisation to agree to cooperate in order for the EU DPA Panel to gain jurisdiction. It was not sufficient to merely indicate the existence of the Panel or to refer consumers with disputes to individual EU Data Protection Authorities.

The agreement to cooperate with the EU DPA Panel may appear in either the self-certification entry or in the privacy policy. As usual there are considerable problems with data quality regarding this requirement. This includes inconsistency between the entry in the form, and entries on privacy policies. Also, 208 organisations failed to click on a selection in this part of the form, so their entry reads ‘select appropriate response’ – it is therefore unclear whether these organisations are bound.

Also, most privacy policies do not accurately convey information about the Panel to consumers. There is often no mention at all of the existence of the Panel. Where EU Data Protection Authorities are mentioned at all, the situation is often misdescribed in terms similar to the following:

If you cannot resolve the issue directly with the Company X Safe Harbor Privacy Contact, you may contact your local data protection authority for further information.¹⁶

Without a clear indication to consumers that the EU DPA Panel exists as an independent dispute resolution service AND a clear commitment to cooperate with the Panel, organisations are not compliant with the Safe Harbor.

In addition, some privacy policies contain references that would make no sense to a consumer, such as:

For human resources data we have agreed to cooperate with Data Protection Authorities.

In this example (and similar sites) there is no information about who or where these data protection Authorities are, and what their role is in the case of a dispute.

Overall, the Galexia study found that there was a very low level of compliance with the requirement to identify the EU DPA Panel correctly as the appropriate dispute resolution provider. Only four organisations in the entire study provided contact details for the Panel.

¹⁶ <<http://www.rrdonnelley.com/wwwRRD1/PrivacyPolicy.asp>>

5.9. Categories of data protected

It is important to note that even if an organisation is compliant with the basic Safe Harbor requirements, they may have limited the scope of their Safe Harbor membership to specific categories of data. This limitation may or may not appear in their published privacy policy, but it is usually recorded in their self-certification entry.

Of the 348 organisations who were found to be compliant in this study, only 54 extended their Safe Harbor membership to all data. Out of the 1,597 entries on the Safe Harbor list only 54 are compliant with basic Safe Harbor requirements for *all* categories of data.

The following table summarises the categories of data selected by the 348 compliant organisations:

Category of Data	Selected	Unique Selection ¹⁷
Human Resources	152	41
Online	294	75
Offline	181	4
Manual	134	2
Other	6	6

6. Recommendations

This study has found that there has been little improvement in either compliance or data quality since the negative 2002 and 2004 EU reviews of the Safe Harbor. Indeed, the growing number of false claims made by organisations regarding the Safe Harbor represent a new and significant privacy risk to consumers.

If the Safe Harbor is to operate effectively, an immediate program of improvements is required.

6.1. Recommendations for the EU

The EU is a significant stakeholder in the operation of the Safe Harbor – it is the personal information of European citizens that is ultimately at risk. The EU should take a more ‘hands-on’ approach to ensuring that the Safe Harbor is providing basic privacy protection:

- The EU should consider re-negotiating the Safe Harbor arrangement so that all member privacy policies are made available on a public website, or posted on the Department of Commerce website, as a minimum entry requirement to the Safe Harbor;
- The EU should consider re-negotiating the Safe Harbor arrangement so that Safe Harbor members are required to select dispute resolution providers that are affordable for ordinary consumers;

¹⁷ ‘Unique selection’ indicates organisations who *only* selected this category of data.

- The EU should consider providing warnings to EU consumers and businesses regarding public claims that an organisation is a member of the Safe Harbor. EU consumers and businesses will need to check the actual membership in order to avoid false claims (currently 206 organisations). This warning will need to instruct EU consumers and businesses to check the certification dates, as the Department of Commerce record of currency is not accurate; and
- The EU should consider undertaking a comprehensive review of all entries on the Safe Harbor list. This could include collecting each privacy policy and assessing it against all seven EU Safe Harbor principles.

6.2. Recommendations for the US

The US should consider taking steps to rectify some of the more pressing Safe Harbor problems identified in this study:

- The Federal Trade Commission and/or the Department of Commerce should consider investigating the hundreds of organisations who make false claims in relation to their membership of the Safe Harbor and/or their membership of dispute resolution providers;
- The Federal Trade Commission and/or the Department of Commerce should consider investigating organisations who claim that they have been certified by the Department of Commerce or certified by the EU, or who otherwise misdescribe the self-certification process;
- The Department of Commerce should consider revising its public statements about the number of organisations who are ‘participants’ in the Safe Harbor at any given date, in order to exclude non-current members, duplicate entries etc.;
- The Department of Commerce should consider investigating the unauthorised and/or misleading use of its Departmental logo in the privacy policies and websites of organisations;
- The Department of Commerce should consider abandoning the use of the Safe Harbor Certification Mark, as it is open to abuse and in the majority of cases it is misleading. Alternatively, the Certification Mark should use the words ‘self certified’ within the graphic, and the graphic should accurately indicate the categories of data covered by that specific organisation’s membership;
- Some Safe Harbor dispute resolution providers (notably DMA) should publish public lists of their members so that membership can be validated by the public (most providers already comply with this requirement);
- All Safe Harbor dispute resolution providers (e.g. TRUSTe, BBB and DMA) should develop a process that automatically suspends an organisation’s membership if they fail to renew their Safe Harbor certification; and
- TRUSTe should require all of its members to immediately cease referring to TRUSTe as ‘non-profit’.

Until the Safe Harbor is reviewed and improved, consumers and business should approach all claims made regarding the Safe Harbor with great care, and undertake their own investigations before providing any personal information to US organisations.

The ability of the US to protect privacy through self-regulation, backed by claimed regulator oversight is questionable. There are growing calls, including campaigns by leading business groups, for the US to abandon the self-regulation approach and embrace comprehensive privacy legislation. Comprehensive privacy legislation ensures that personal information is protected by privacy rights for all organisations, all of the time. Where legislation is in place an individual’s privacy rights do not disappear because an organisation has forgotten to renew their membership of a dispute resolution service, or because a dispute resolution service closes its doors.

The International Monetary Fund (IMF) publishes a list of advanced economies – those economies that have advanced markets, high wealth and do not rely on a single resource such as oil. Of the 31 countries that appear on that list only Singapore and the US do not have privacy legislation. It may be time for the US to abandon one list and join the other.

7. Appendix – Methodology for this study

The study methodology is summarised in the following table:

Step	Task	Notes
1	Capture raw data	All 1,597 entries were downloaded on 17 October 2008.
2	Check for doubles	19 organisations were listed more than once or appeared in the list under multiple names.
3	Check currency	Organisations were categorised as not current if their status in the list had been marked as not current by the Department of Commerce and/or their date for renewal of certification had passed.
4	Find privacy policies	Privacy policies were accessed using the direct links provided in the list and / or the home URL of the organisation. This step required numerous additional steps to correct typos, search websites etc.
5	Check privacy policies for mention of the Safe Harbor	Privacy policies were searched for 'Safe Harbor', 'Europe' and variations of these terms.
6	Check privacy policies for compliance with Principle 7 – Enforcement	Privacy policies were searched for 'dispute', 'complaint', 'panel' and variations of these terms. The relevant sections of the policy were then assessed against the requirements of Principle 7.
7	Check website for seals and trustmarks	Websites were checked for relevant seals and trustmarks, including both authorised and unauthorised Department of Commerce seals, and private sector trustmarks such as TRUSTe, BBB and DMA.
8	Check validity of trustmarks	Where possible the validity of trustmarks was cross checked against lists maintained by private sector trustmark providers (only TRUSTe and BBB Safe Harbor maintain public lists).
9	Quality control	The study re-checked the 'not current' status of organisations. As the study took 4 weeks to complete a small number of entries were updated as organisations had renewed their certification.