Guidelines for Privacy Policymakers

DEVELOPED BY THE PUBLIC POLICY DIVISION OF THE
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

Copyright © 2016. All rights reserved.

Table of Contents

SIIA is an umbrella association representing 800+ technology, data, and media companies globally. Industry leaders work through SIIA's divisions to address issues and challenges that impact their industry segments with the goal of driving innovation and growth for the industry and each member company. This is accomplished through in-person and online business development opportunities, peer networking, corporate education, intellectual property protection, and government relations. For more information, visit siia.net.

Introduction

These guidelines are intended for government officials who are responsible for developing, adopting and implementing measures to protect consumer privacy. They should also be of use to company and institutional privacy officers seeking to establish good practices within their organizations with respect to personally identifiable information. Lastly, they should be of interest to commentators, scholars and advocates seeking to understand and change consumer privacy policy.

Many privacy policymakers accept the idea that privacy is a fundamental human right. Indeed, privacy is listed as a fundamental human right in many international human rights treaties, along with security, free speech and the right not to be tortured. Privacy as a fundamental right is contained in the treaties that form the constitutional structure of the European Union. [1] The recently adopted EU General Data Protection Regulation, like its predecessor the 1995 Data Protection Directive, is explicitly designed to implement this idea of privacy as a fundamental human right.[2]

But what are the practical implications of thinking of privacy as a fundamental human right? Often, it is thought that embracing privacy rights means embracing the entirety of the fair information practices as these principles have been articulated in successive iterations starting with their original expression in 1973. These principles include notice, choice, access and security as well as purpose specification, data minimization, use limitation, data quality and integrity, and accountability and auditing. [3]

In the United States this line of thinking leads to the idea that we should adopt a uniform consumer privacy bill of rights containing a version of the fair information practices. [4]

These guidelines take a different approach. They do not require the adoption of a comprehensive system of privacy principles such as the European Union's General Data Protection Regulation or a proposed consumer privacy bill of rights, but they can be of use to policymakers seeking to implement a comprehensive system. They can also assist policymakers seeking to legislate or regulate in a specific area such as drones, student privacy, information service providers, or broadband privacy.

They start with the practical problems faced by regulators attempting to protect privacy rights. This practical focus makes it easy to see how and why effective privacy protection does not always require imposing all the fair information practices as universal responses to privacy problems. Sometimes notice and choice makes sense. Sometimes they are not needed. Sometimes data controllers should discard information as soon as possible; sometimes it makes sense for them to retain it longer. Sometimes an access requirement is needed to protect people; sometimes it is not.

Privacy laws and regulations usually pick and choose among the fair information practices to solve practical problems. Even comprehensive privacy laws, such as the EU's General Data Protection Regulation, provide for numerous exceptions and limitations on the fair information practices it

adopts. But what is the basis for these choices and exceptions? When does it make sense to apply one of the principles? When to create an exception? When to take a different approach entirely?

These guidelines are an attempt to answer these practical questions. In some cases, they involve rethinking a principle such as data minimization. In other cases, they suggest factors to consider when determining whether or how to apply one of the principles. They should be of use to all privacy policymakers, including those who believe privacy is a fundamental right or who are charged with implementing laws based on that assumption.

Summary

Privacy policy makers can use two approaches in determining in practice what the demands of privacy are. A consequentialist framework focuses on the likely outcome of a proposed privacy requirement and uses an assessment of benefits and costs to decide when and how to regulate. [5] A contextualist approach treats privacy as a collection of informational norms tied to specific contexts like medicine, education, or finance and regulates to maintain or enforce these privacy norms.[6]

The following guidelines incorporate valuable elements from each of these approaches:

1. Focus on Consequences. Privacy regulators should rely on careful analysis of the consequences of their decisions and adopt a regulation only upon a reasoned determination that its benefits justify its costs.
2. Look for Specific Injuries. Any new privacy measures should be targeted to mitigate significant risks of specific injuries.
3. Context Matters. Privacy norms and expectations differ by context. Regulatory requirements that make no sense in some social and business contexts might be needed in others, and vice versa.
4. Technology Matters. Regulatory principles need to be evaluated in light of the developments in new technology such as artificial intelligence, machine learning, cloud computing, big data analytics and the Internet of Things.
5. Pick the Right Regulatory Tool for the Job. Fair information practices set out a range of regulatory tools that can be deployed to address specific injuries, but not every principle needs to be required to solve a specific problem.
6. Transparency and Targeted Consumer Notices. Transparency promotes consumer trust. Notice is especially important when consumers have a concrete decision to make and need the information to make an informed choice or to take steps to protect themselves.
7. Design Choice Architecture Carefully. Opt-in might be needed when an information practice is extremely likely to result in injury, but often opt-out can effectively protect privacy rights.
8. Encourage De-Identification. Regulators should provide incentives to use de-identified data sets when analytical purposes can be accomplished without identifying information.
9. Data Minimization Should Be Risk-Based. Data sets in identifiable form should be discarded or de-identified only when there are significant foreseeable risks and little anticipated benefit in retaining them.
10. Secondary Use Should Avoid Injury and Provide Benefits. Information collected for one purpose should not be used for a secondary purpose that is likely to impose significant

injuries on the data subject or others. Secondary use that is inconsistent with context should be permitted when it provides benefits to the data subjects or others.

Guidelines

1. Focus on Consequences

Privacy regulators should rely on careful analysis of the consequences of their decisions and adopt a regulation only upon a reasoned determination that its benefits justify its costs.

Every U.S. administration since the Carter Administration, Republican and Democratic, including the Obama Administration has embraced the philosophy of setting and reviewing regulations on the basis of evidence and data regarding their likely consequences.[7] This general approach should apply to consideration of new privacy regulation.

Leading privacy law scholars have also embraced this focus on consequences. Paul Ohm says: "Before enacting any privacy law, lawmakers should weigh the benefits of unfettered information flow against its costs and must calibrate new laws to impose burdens only when they outweigh the harms the laws help avoid."[8] Daniel Solove says: "We should understand the value of privacy in terms of its practical consequences. Privacy should be weighed against contrasting values and it should win when it produces the best outcome for society."[9]

This does not mean that privacy has to be quantified. Many real effects of information practices such as the benefits of increased autonomy and opportunity or the injury of an affront to human dignity are not amenable to expression in quantitative terms. A qualitative but rigorous assessment might be all that is possible in many cases.

Regulators who think of privacy as a fundamental right must still focus on consequences in order to implement the right to privacy, as is the case for all fundamental or statutory rights. Courts implement constitutional free speech and equal protection rights by assessing whether a government rule is a narrowly tailored means to achieve a substantial government interest.[10]

Courts and regulatory agencies implement statutory rights to non-discrimination in employment and housing through fact-based disparate impact analyses that ascertain whether an adverse impact on a protected class has a business justification and whether that business objective can be obtained through a less impactful means.[11] Regulators implement statutory rights to safety and health on the job and to a clean environment by ascertaining how much their measures in fact advance worker safety or clean air and whether there are more efficient ways to accomplish the same goals. The only practical way to implement rights is to focus on consequences.

The Federal Trade Commission's notion of unfairness provides a good framework for regulators to use to focus on consequences. The FTC takes action against "unfair" acts or practices and defines an act or practice as unfair when it "causes or is likely to cause substantial injury to consumers which is

not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[12] It has used this authority in a diverse range of cases to protect consumers against the injuries from data and privacy breaches.

2. Look for Specific Injuries

Any new privacy measures should be targeted to mitigate significant risks of specific injuries.

New developments in technology and institutions can pose significant privacy risks to consumers, students, patients, employees and the general public. Unconstrained information uses can cause intrusion, identity theft, and unfair or discriminatory denial of employment, credit or insurance, among other social ills. The primary practical duty of privacy regulators is to identify areas where the use of information is highly likely to have specific adverse consequences and then devise realistic remedies to mitigate these risks.

But what is an injury, an adverse consequence? The consumer injuries that the FTC focuses on are a good place to start. Its notion of an unfair practice as one that causes or is likely to cause substantial injury to consumers is an important guide.

Other statues provide guidance as well. People who are denied employment, credit or insurance because of the use of inaccurate, outdated or irrelevant information have been harmed. To prevent this type of harm, the Fair Credit Reporting Act (FCRA) sets out extensive consumer rights and company responsibilities regarding the use of information for determining eligibility for insurance, credit or employment.[13]

People are also injured by the use of personal information for invidious discrimination. Existing antidiscrimination laws ban this form of injury. For instance, Title VII of the Civil Rights Act of 1964 makes it unlawful for employers and employment agencies to discriminate against an applicant or employee because of such individual's "race, color, religion, sex, or national origin."[14]

Privacy regulators need to pay special attention when an information use creates substantial risks of material and tangible harms such as financial loss, reduced eligibility status for employment, insurance or credit, or threats to safety and health. These are recognized and understood as substantial injuries.

What about subjective injuries such as feelings of mental distress, embarrassment, humiliation or anguish brought on by perceived privacy invasions? Here privacy regulators must be careful, for they cannot validate every idiosyncratic feeling of privacy wrong.

One model for proceeding is the Supreme Court's standard of reasonable expectations of privacy under the Fourth Amendment. The Court examines the extent to which people's actual expectation of privacy is "one that society was prepared to recognize as 'reasonable.'"[15] The notion of "reasonableness" is intrinsically tied to entrenched social norms of appropriate information flow.

A similar "reasonableness" test can be found in the case law of privacy torts. For instance, plaintiffs alleging an intrusion upon solitude or seclusion can recover damages not merely when the activity

offends them but when it would be "offensive to a reasonable person," that is, when it transgresses a social norm whose violation would properly be viewed with outrage or affront.[16]

The FTC's Do Not Call rule illustrates how this "reasonableness" test can work. The FTC identified a specific activity – the intrusion of unsolicited telemarketing calls – as an injury that consumers were entitled to control, noting that it was an "abuse" that "consumers continue to be angered by and frustrated with the pattern of unsolicited telemarketing calls they receive from the multitude of sellers and telemarketers."[17] Outrage and affront against telemarketing calls were not isolated idiosyncratic, arbitrary responses, but an appropriate reaction to the violation of a widely shared entrenched social norm. The Do Not Call rule was aimed at providing a mechanism to allow consumers to protect themselves against this specific injury.

3. Context Matters

Privacy norms and expectations differ by context. Regulatory requirements that make no sense in some social and business contexts might be needed in others, and vice versa.

Policymakers should examine whether information practices are in accordance with entrenched context-specific informational norms and consider whether new policies are needed to maintain these norms. If an information practice violates entrenched informational norms, it is likely to prompt widespread feelings of affront and outrage. For example, patients would be rightly angry if their doctor used their medical records for personal gain such as making them available to a marketing firm. This particular kind of injury is addressed in the medical privacy regulation under the Health Insurance Portability and Accountability Act.[18]

An information practice inconsistent with context can also interfere with the proper functioning of social contexts. This kind of contextual harm can arise, for instance, when people avoid getting genetic tests in order to protect themselves from adverse judgments about employment or insurance eligibility, thereby impeding the practice of public health and medical research.[19]

On the other hand, when an information use is well established, understood by all participants and part of an ongoing social practice, there is little need for regulators to consider regulatory measures related to that use. People expect merchants to use their credit card information to complete their transactions, and use their address to deliver the products they order. Why give special notice of these practices to data subjects and require them to consent to these context-appropriate information uses? Consistency with general community expectations and norms signals the lack of any injury for the regulator to mitigate.

This approach has increasingly been incorporated into privacy policymaking. The Federal Trade Commission, the Obama Administration, the new EU General Data Protection Regulation and the Federal Communication Commission's proposed privacy rules for broadband providers all have a key role for consistency with context.[20]

Understanding the informational norms present in a particular social context is an excellent first step in examining whether an information practice is problematic. Inconsistency with context might even create a presumption against an information practice. But it is a rebuttable presumption that can be overcome when a new information practice is beneficial. For instance, as Helen Nissenbaum points out, it makes sense to adopt technical improvements in education that are not in accordance with traditional informational norms when the new technology improves student learning, thereby promoting the goals, values and purposes of education. [21]

In general, new information practices might be improvements over traditional ways of doing things. People might not expect a novel information practice, but might welcome it once it is available. As Dan Solove writes, "Privacy is not just about what people *expect* but about what they *desire*."[22]

4. Technology Matters

Regulatory principles need to be evaluated in light of the developments in new technology such as artificial intelligence, machine learning, cloud computing, big data analytics and the Internet of things.

Policymakers sometimes need to adapt privacy principles in the face of significant technological changes. They need to evaluate and possibly revise them to protect against new threats to privacy or to allow for the successful realization of new possibilities for social gain created by technological advances.

History verifies this point. In the 1890s, Warren and Brandeis developed the right to privacy as the right to be left alone in reaction to the development of the snap camera and mass print media. Sixty years of case law produced Prosser's four privacy torts as a systematization of the harms from different privacy invasions.[23]

These legal structures proved inadequate to deal with the arrival of the mainframe computer which allowed the collection, storage and processing of large volumes of personal information to improve operations in business, government and education. A regulatory paradigm of fair information practices arose to fill this gap. [24]

Today, artificial intelligence, machine learning, cloud computing, big data analytics and the Internet of Things rest firmly on the ubiquity of data collection, the collapse of data storage costs and the astonishing power of new analytic techniques to derive novel insights that can improve decision making in all areas of economic, social and political life. A reevaluation of regulatory principles is needed in light of these new technologies.

This is not to say that each new technology deserves its very own set of privacy rules. Sometimes a shorthand label such as the "Internet of Things" misleadingly suggests the presence of a single new technology that might be separately regulated. Privacy policymakers should focus on the risks and benefits that new technology makes possible in particular social and business contexts.

For instance, in an earlier technological age, policymakers could successfully protect privacy by a universal data minimization rule, since it reduced privacy risks and sacrificed no social gains at all. However, in an age of big data this rule would sacrifice considerable social gains. It needs to be rethought.

5. Pick the Right Regulatory Tool for the Job

Fair information practices set out a range of regulatory tools that can be deployed to address specific injuries, but not every principle needs to be required in order to address a particular injury.

In the Do Not Call rule, the FTC provided an easy, convenient opt-out that allowed consumers disturbed by the privacy intrusion of telemarketing calls to stop them. It considered banning the practice, but recognized that some consumers valued the information from telemarketing calls. It considered an opt-in, but thought that was more than was necessary to allow consumers to stop an offensive activity. It did not try to stop the sharing of telephone information with third parties, or create an access requirement on telemarketer databases. It did not impose data retention limits or data minimization requirements on any party. Instead, the agency designed a limited, focused choice mechanism and nothing else. The regulation was spectacularly successful: more than 200 million telephone numbers are on the Do Not Call list.

This illustrates that not every tool in the regulators toolbox needs to be used for every job. It is prudent to find the regulatory measure that best responds to the specific problem at hand.

To take another example, the Fair Credit Reporting Act was aimed at ensuring that applicants for employment, credit, and insurance were not harmed by the use of inaccurate, outdated or irrelevant information. But legislators rejected choice as a regulatory tool, since it would make credit reporting impossible. Instead, they imposed targeted rights and requirements including notices of adverse actions and a right of access and correction.

Information security provides a third example. The FTC needed to respond to the specific injuries such as identify theft created by data breaches of credit card and other financial information. In crafting its response, the FTC did not demand disclosure to consumers of security practices or levels of security. It did not require consent opportunities for consumers, or seek limitations on company collection or use of personal information. Instead, it brought cases alleging that companies with poor security practices who had suffered a data breach were guilty of an unfair practice. This implicit requirement that companies adopt reasonable security practices was a targeted, narrow and effective response to a specific problem.

6. Transparency and Targeted Consumer Notices

Transparency promotes consumer trust. Notice is especially important when consumers have a concrete decision to make and need the information to make an informed choice or to take steps to protect themselves.

Transparency about their information practices is often the best way for companies to gain consumer trust. When companies collect personal information directly from consumers they generally have an obligation to inform the consumers what information they collect, what they do with it, and what choices if any consumers have with respect to its use. When they significantly change what they do with personal information, they should disclose the changed information

practice to their customers. Without these disclosures, consumers have no way to assess whether they want to do business or to continue to do business with the companies.

But over notification is a real danger.[25] Universal notice about all information collection and use will overwhelm consumers and accomplish no good purpose. Consumers need not be told, for instance, which intermediary payment processor a merchant is using to manage credit card transactions, nor do they need to know the details of the security measures taken to protect their information. In fact, almost all of the information transfers and processing that go on behind the scenes of everyday life are and should remain invisible to ordinary consumers.

Notice is especially important when consumers have a concrete decision to make and need the notice to make an informed choice. This is essential in the "take it or leave it" variety of choice, where the ability to obtain a service is conditioned on accepting the provider's information policy. In these cases, clear, specific, conspicuous notices need to be provided in a form and at a time where the consumer can use the information to make the informed choice.

Notice is also particularly important when consumers are uniquely situated to assess injury and to take steps to protect themselves. Data breach notification measures fall into this category. When a data breach creates a significant risk of identity theft or other financial harm, consumers can protect themselves by flagging their credit files and checking their credit reports frequently. But they can do this only if they receive timely and accurate notices. Data breach notification thereby gets crucial information into the hands of consumers when they can use it to protect themselves from specific injuries.

7. Design Choice Architecture Carefully

Opt-in might be needed when an information practice is extremely likely to result in injury, but often opt-out can effectively protect privacy rights.

Information choice architecture is inevitable - some rule or practice will govern what choices if any consumers have over the collection and use of their personal information. Privacy regulators have three options in this area. They can allow private companies to select the choice options available to consumers with no regulatory requirement at all. They can require companies to provide consumers with an opportunity to opt out of information practices. Or they can require companies to obtain affirmative explicit consent from data subjects for information use to proceed.

Often, the first alternative of no regulatory mandates makes the most sense, because a required opt-in or opt-out process would be unnecessary or counterproductive. Privacy policymakers often take this road:

- FTC guidance is that choice is not needed for commonly accepted business practices.[26]
- Financial privacy legislation exempts fraud protection and risk reduction from notice and choice requirements. [27]
- To preserve the integrity of the system, consumers do not have a choice about what information goes into their credit reports.[28]

- Drivers cannot prevent highway officials from using driver identification information for highway or motor vehicle purposes.[29]
- Parents cannot tell schools not to gather or share student information for educational purposes.[30]
- Patients cannot block the flow of health information among health care providers for treatment purposes.[31]
- The FCC's proposed broadband privacy rules would allow no choice at all for routine uses of information such as network routing and billing.[32]

In general, regulators should not aim to maximize the number of privacy choices people have as if more choice were always a good thing. They should refrain from mandating choice options for data subjects when the choice is obvious from the context or when allowing choice would dissipate an important public benefit, or where there is no discernible harm in allowing a "take it or leave it" consumer offering.

When regulators need to intervene in this area, should they set the default as opt-in or opt-out? Even when people can change the default, most people do not. So, picking the default is a "nudge" that has substantial implications for individual and collective welfare.[33]

In other contexts of designing choice architecture outside of privacy regulation, policymakers have aimed to set the default as the option that rational agents seeking to maximize their welfare would select if they had complete information and unlimited cognitive abilities. Privacy regulators might consider this kind of soft paternalism in their own regulatory activity.

Context and consequences are also ways to structure decisions about imposing opt-in versus opt-out choice. In the contextual approach, when an information use is surprising or unexpected, opt-in might be the right way to go. The consequentialist approach would say that opt-in makes sense if the consequences of an information use are especially risky. Otherwise, opt-out is sufficient.

The FTC provided a nice example of how to use both context and consequence in their discussion of choice for sensitive information. They noted that "affirmative express consent is appropriate when a company uses sensitive data for any marketing." But they also said that this requirement is limited, and does not apply to "general audience businesses that incidentally collect and use sensitive information" because "the risks to consumers may not justify the potential burdens." [34]

The wrong selection of choice architecture can have significant effects. For instance, if regulators had required affirmative consent for subscriber listing in telephone books, few people would have taken the effort to opt-in with the result that there would have been no economic incentive to publish telephone directories. However, an opt-out was enough to provide concerned subscribers with a mechanism to keep their phone numbers private.

The FTC's Do Not Call rule has a similar lesson for privacy policymakers deciding between opt-in and opt-out. Sometimes an easy convenient opt-out is enough for people who are concerned about a

privacy issue. The FTC chose opt-out for its Do Not Call rule and it is one of the most popular regulations of all time, with over 200 million phones signed up to block telemarketing calls.

It might seem as though this choice discussion concerns only the U.S, since the European framework bars opt-out as a way of providing consent. The General Data Protection Regulation requires consent to be affirmative and opt-in. But consent is not the only ground for lawfulness under the regulation. Processing is also lawful when it is "necessary for the purposes of the legitimate interests pursued by the controller…" provided the data subject has not objected.[35] So the European framework provides for opt-out choice through the provision of a right to object. The question of opt-in or opt-out also arises in the European context.

8. Encourage De-Identification

Regulators should provide incentives to use de-identified data sets when analytical purposes can be accomplished without identifying information.

Many of the benefits of big data analytics do not require identifiable databases at all. One medical study of pre-mature babies revealed an unexpected early indicator of impending fever - vital signs flat line twenty-four hours before the fever onset. The study needed individual-level data but not identifiable data.[36]

Many such insights are possible using de-identified data sets and should be encouraged. The FTC is on the right track by exempting de-identified databases from its recommended privacy rules.[37]

9. Data Minimization Should Be Risk-Based

Data sets in identifiable form should be discarded or de-identified only when there are significant foreseeable risks and little anticipated benefit in retaining them.

Before the introduction of credit cards using a chip, a common way to make a counterfeit card was to hack into a merchant database in the hopes of finding the right information. If the database contained the access codes that had been read from the card's magnetic stripe, then the thieves could make the counterfeit cards, but without this code a fake card would not work at the point of sale. This led to a very simple security rule: don't store the access code. There was no business reason for it to be retained and substantial risk.

That's a model for data minimization in an age of big data. With the increasing capacity of big data analytics to derive new insights from old data, the principle of collecting the minimum amount of information and throwing it away as soon as possible is no longer appropriate. However, in exceptional cases such as the credit card example above, retaining information could create an unnecessary risk of harm. In these cases, data controllers should assess the likely harm in retaining the data compared to the likely gains and throw away information or de-identify it when the risks of harm are too great.

10. Secondary Use Should Avoid Injury and Provide Benefits

Information collected for one purpose should not be used for a secondary purpose that is likely to impose significant injuries on the data subject or others. Secondary use that is inconsistent with context should be permitted when it provides benefits to the data subjects or others.

Often information gathered for one purpose is found to be useful for additional purposes. Health information gathered for the purpose of treatment has enormous value for medical research. Information used to assess student learning progress can also be used to examine the effectiveness of new educational tools and programs. Information on automobile purchases in an area can guide decisions on what parts to stock in auto supply stores. Location information needed to pick up and deliver cell phone calls and emails can also be used in the aggregate to describe and predict traffic patterns.

An unrestricted secondary use principle would call for stringent privacy controls for all uses that are unrelated to or different from the original purpose of data collection and processing. But this is too strong. It creates procedural barriers to beneficial uses of information that are not justified by either a contextual analysis or by an analysis of harm. In general, secondary uses of personal information are legitimate when they do not pose a significant risk of harm to the data subject or when they are consistent with the context of information collection and use.

A modified principle, however, could make sense in certain circumstances. When the additional use of personal information is substantial, disclosure to the data subjects might be appropriate. When there is a significant risk of injury to data subjects, an appropriate level of control might be needed – prohibition, opt-in or opt-out, depending on the severity of the risk. When the new information use is surprising or unexpected, it should provide some benefits to the data subject or to the broader public.

If a statutory or regulatory standard for secondary use is compatibility with the original purpose of data collection, as is the case in the European General Data Protection Regulation, then this analysis of context and likelihood of harm should be key elements in assessing whether the new use of the data is compatible with the original purpose. [38]

Endnotes

[1] See Universal Declaration of Human Rights, Article 12 http://www.un.org/en/documents/udhr/ ; International Covenant on Civil and Political Rights, Article,17 http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf; European Convention on Human Rights, Article 8(1) http://www.echr.coe.int/Documents/Convention_ENG.pdf; Treaty on the Functioning of the European Union, Article 16 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN; Charter of Fundamental Rights of the European Union, Articles 7 and 8 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

[2] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 1(2): "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOCotn

[3] Robert Gellman, Fair Information Practices: A Basic History available at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

[4] Executive Office of the President, Consumer Data Privacy in A Networked World: A Framework for Protecting Privacy and Promoting Innovation in The Global Digital Economy February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[5] J. Howard Beales, III & Timothy J. Muris, "Choice or Consequences: Protecting Privacy in Commercial Information," 75 U. Chi. L. Rev. 109 2008 especially pp. 109-120 available at https://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/75.1/75_1_Muris_Beales.pdf

[6] Helen Nissenbaum, Privacy in Context, Stanford University Press, 2009

[7] The Obama Administration continued this tradition, applying a cost-benefit approach directly to executive agencies in Executive Order 13563 of January 18, 2011, "Improving Regulation and Regulatory Review," https://www.whitehouse.gov/sites/default/files/omb/inforeg/eo12866/eo13563_01182011.pdf p. 3821 and recommending a focus on consequences for independent agencies like the FTC and the FCC in Executive Order 13579--Regulation and Independent Regulatory Agencies July 11, 2011 https://www.whitehouse.gov/the-press-office/2011/07/11/executive-order-13579-regulation-and-independent-regulatory-agencies. The key ideas are that "Wise regulatory decisions depend on…careful analysis of the likely consequences of regulation" and that agencies should "…adopt a regulation only upon a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify)."

[8] Paul Ohm, "Broken Promises of Privacy: Responding to The Surprising Failure of Anonymization," 57 UCLA Law Review 1701 (2010), p. 1736 at http://www.uclalawreview.org/pdf/57-6-3.pdf

[9] Daniel Solove, Understanding Privacy, Harvard University Press, 2008, p. 87

[10] See, for instance, United States v. O'Brien, 391 U.S. 367,368 (1968) holding that a government regulation passes First Amendment review when it furthers "…an important or substantial governmental interest unrelated to the suppression of free expression, and if the incidental restriction on alleged First Amendment freedom is no greater than is essential to that interest."

[11] For disparate impact in housing see the Fair Housing Act (24 C.F.R. § 100.500) which says that a business practice has a prohibited discriminatory effect "where it actually or predictably results in a disparate impact on a group of persons . . . because of race, color, religion, sex, handicap, familial status, or national origin," and it is either not "necessary to achieve one or more substantial, legitimate, nondiscriminatory interests," or any such interests "could be served by another practice that has a less discriminatory effect." For disparate impact in employment, see Title VII of the Civil Rights Act of 1964 (42 U.S.C. § 2000e-2(k)(1) which forbids any employment practice that causes a disparate impact on a prohibited basis if the practice is not "job related for the position in question and consistent with business necessity" or if there exists an "alternative employment practice" that could meet the employer or employment agency's needs without causing the disparate impact.

[12] Federal Trade Commission Act, 15 U.S.C. 45(n) (2006).

[13] 15 U.S.C. § 1681a available at http://www.law.cornell.edu/uscode/text/15/1681a

[14] 42 U.S.C. §2000e-2 available at http://www.law.cornell.edu/uscode/text/42/2000e-2
[15] Katz v United States 389 U.S. 347 (1967)
[16] Robert C. Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989). *Faculty Scholarship Series.* Paper 211.
http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1210&context=fss_papers
[17] Federal Trade Commission, Telemarketing Sales Rule, 68 Fed Reg 4580 (2003) p. 4631 available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-congress/dnciareportappenda.pdf
[18] Department of Health and Human Services, Summary of the HIPAA Privacy Rule available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html;
[19] National Genome Research Institute, Genetic Discrimination, available at http://www.genome.gov/10002077
[20] The Federal Trade Commission recommends that for practices inconsistent with the context of their interaction with consumers, companies should give consumers choice, but that companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices. See Federal Trade Commission, Protecting Consumer Privacy in an Age of Rapid Change, March 2012 (FTC Report), p. 36 and 48, available at athttps://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. The Obama Administration recommended a consumer privacy bill of rights containing a principle calling for "Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." See Executive Office of the President, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, February 2012, p. 15 available at https://www.whitehouse.gov/sites/default/files/privacy-final.pdf The new European General Data Protection Regulation calls for consideration of "the context in which personal data have been collected" in determining whether further use of information is compatible with the purpose for which the data were originally collected. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 6(4)(b) available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOCotn. In addition, the GDPR recognizes the importance of considering context in assessing when legitimate interests of a controller may provide a legal basis for processing, by saying, "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller." GDPR, Recital 47. The Federal Communications Commission's proposal for broadband privacy, calls for opt-out consent for marketing communications-related services, but opt-in consent for other uses because they think that this approach is "consistent with consumer expectations" and observes the regulatory best practice that "consumer choice turns on the extent to which the practice is consistent with the context of the transaction." See Federal Communications Commission, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Notice of Proposed Rulemaking, April 1, 2016, (FCC Broadband Privacy) p. 44, available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0401/FCC-16-39A1.pdf.
[21] Nissenbaum, Privacy in Context, p. 169-171
[22] Daniel J. Solove, "The Meaning and Value of Privacy," in *Social Dimensions of Privacy: Interdisciplinary Principles*, ed. Beate Roessler and Dorota Mokrosinska Cambridge University Press, 2015, p. 76.
[23] See Paul Ohm's short history of the Evolution of Privacy Law, pp. 1731-1739 in "Broken Promises."
[24] Robert Gellman, Fair Information Practices: A Basic History available at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf
[25] The FCC warns against "notice fatigue" and asserts that good notice practices do not require "bombarding (consumers)with constant solicitations for approval." Broadband Privacy, NPRM, p. 39
[26] FTC Report, p. 48

[27] Title V of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§6801–09
[28] Fair Credit Reporting Act of 2003, 15 U.S.C. § 1681
[29] Driver's Privacy Protection Act of 1994, 8 U.S.C. § 2721
[30] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g
[31] Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 C.F.R. 164.524(a)(1)(ii) available at https://www.gpo.gov/fdsys/pkg/CFR-2015-title45-vol1/xml/CFR-2015-title45-vol1-sec164-502.xml
[32] FCC Broadband Privacy, p. 9.
[33] Richard H. Thaler and Cass R. Sunstein, Nudge: Improving Decisions about Health, Wealth, and Happiness, Yale University Press, 2008
[34] FTC Report, pp. 47-48 https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
[35] Article 6(1)(f) of the General Data Protection Regulation, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOCotn
[36] Viktor Mayer-Schonberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think, Houghton, Mifflin Harcourt, 2013, p. 61
[37] The Commission exempts a data base when a company has reasonably de-identified the data base, committed to not attempting to re-identify data subjects, and requires third-parties who access the data base to abide by similar restrictions. See Federal Trade Commission, Protecting Consumer Privacy in an Age of Rapid Change, March 2012, p. 21, available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
[38] Europe's standard is whether the additional use is compatible with the purpose for which the data were initially collected. But in making this determination the data controllers must take into account context and consequences. See General Data Protection Regulation, Article 6(4), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOCotn

The Software & Information Industry Association (SIIA) is an umbrella association representing 800+ technology, data, and media companies globally. Industry leaders work through SIIA's divisions to address issues and challenges that impact their industry segments with the goal of driving innovation and growth for the industry and each member company. This is accomplished through in-person and online business development opportunities, peer networking, corporate education, intellectual property protection, and government relations.
For more information, visit siia.net.

Copyright © 2016. All rights reserved.

SIIA Public Policy
Software & Information Industry Association
1090 Vermont Avenue NW
Sixth Floor
Washington, DC 20005