3 Privacy and Data Protection

Long before the arrival of Google and Facebook, the impact of computing and communication technologies on privacy presented one of the most significant regulatory challenges of the information age. From the middle of the twentieth century, the use of mainframe computers to process government and company data started to have an impact on individual privacy. This process accelerated in the 1970s as minicomputers and then personal computers became a pervasive part of organizations in advanced economies.

Now, Internet users' browsing, searching, and even e-mailing behavior is routinely profiled by advertising networks and of great interest to law enforcement and intelligence agencies. The nascent "Internet of things" (allowing remote virtual interaction with physical objects) will add billions of sensors to the network, potentially allowing individual behavior in the physical world to be as closely tracked as online activity. Many governments have responded with national laws and international treaties implementing fair information practices to improve the transparency and safeguards associated with the processing of personal data.

Privacy and data protection is a well-studied field—not least because it has proven difficult for legislators and regulators to keep up with the rapid pace of change in Internet technologies that gather, process, and share data related to individuals. In this chapter, we assess more recent attempts to shape the development of Internet technologies in an effort to improve the efficacy of regulation by embedding privacy by design into new systems. These efforts have been led by the EU, while the U.S. government has largely left privacy concerns about business behavior to be met through self-regulation, with limited policing of deceptive practices by the Federal Trade Commission (FTC). Regulation has therefore been driven to some

extent by the interaction between large U.S. Internet companies and EU legislators and national data protection authorities.

Public Policy Objectives

Social Impact of Technology

The impact of new information technologies on privacy has been the subject of intense debate since the development of the portable camera in the nineteenth century. Combined with the relatively new newspaper industry, this created the forerunner of paparazzi photographers and scandal sheets.

In response, Samuel Warren and Louis Brandeis famously described privacy as the "right to be let alone" (1890), emphasized in a later dissenting U.S. Supreme Court opinion by then-Justice Brandeis as "the most comprehensive of rights, and the right most valued by civilized man" (*Olmstead* v. *United States* 1928). But it took decades of widespread telephone use for that Court to decide that constitutional protections against unreasonable searches also applied to telephone conversations (*Katz* v. *United States* 1967).

During the 1970s, governments in North America and Europe developed fair information processing principles designed to protect privacy, as mainframes and minicomputers became widespread in the public and private sectors. The principles were first expressed in the laws of several European nations such as Sweden and France, and in rudimentary form in the U.S. Fair Credit Reporting Act in 1970. They were then agreed at the international level, leading to the OECD Guidelines (1980) and the Council of Europe Convention (CETS No.108 1981). The principles have seen their strongest and most influential expression in the EU (Directive EC/95/46).

However, the Internet and modern computers have presented a significant challenge to data protection regulation. Underlying computing power has been doubling every eighteen to twenty-four months since Intel cofounder Gordon Moore famously observed this relationship in 1965. Bandwidth and storage capacity have been increasing even more quickly. All of this has made it easier than ever before for governments and companies to store, share, and process ever greater quantities of personal data.

Law enforcement and intelligence agencies have, at varying speeds, woken up to the surveillance potential of the digital tsunami of personal

data now being generated by individuals' day-to-day interactions with information systems. Data retention laws passed in Europe (and proposed in the United States) require telephone companies and ISPs to store information about their customers, including details of telephone conversations and e-mail correspondents. Mobile phone companies have detailed data on their customers' location and can carry out real-time tracking of specific individuals. Web sites usually store detailed logs of their users' activities, which can be accessed with varying degrees of judicial oversight in the United States and Europe (Brown 2009). Even offline activities such as buying travel tickets now commonly generate a digital trail, which under bilateral agreements (such as between the EU and Australia, the United States, and other nations) can be automatically shared and stored for a decade or more.

Other government agencies are eager to move services online, both for customer service improvements (such as personalization and immediate delivery) and cost savings. E-government initiatives commonly link up and centralize previously separate databases of personal data across government departments, creating the potential for much more detailed profiling of individual citizens (Anderson et al. 2009).

The United Kingdom has been a leading example of this trend. While prime minister, Tony Blair committed the government to make all services available online by 2005. Initiatives such as national health, identity, and social security databases caused fears of a "database state," with the information commissioner warning that the country was "sleepwalking into a surveillance society" (Ford 2004). This became a significant election issue in 2010, with the winning Conservative and Liberal Democrat parties abolishing Blair's national identity scheme and children's database.

At the same time, an advertising economy has developed on the Internet, whereby most Web sites' business models are based around selling advertising space and clicks. Users remain extremely reluctant to pay for content beyond specialized areas such as financial journalism. Publishers and providers of services such as Web mail, online document editors, and social media (covered in more detail in chapter 6) are eager to deploy technology that increases the effectiveness, and hence revenues, of advertisements. "Behavioral advertising," tailored to profiles built around users' previous browsing behavior, promises to do so—although few data in the public domain show its specific effects.

A second major technological shift underway is the gradual introduction of an Internet of things, where physical sensors such as radio frequency identifier (RFID) tags generate data about real-world objects that are then linked to online databases. RFID has already seen significant deployment, with multinational organizations such as Walmart and the U.S. Department of Defense requiring tags on all supplies to help manage logistics.

RFID and more sophisticated tags are now used in transport payment cards (such as London's Oyster and Hong Kong's Octopus cards) and for low-value payments using credit cards (Visa's PayWave and Mastercard's PayPass standards). These tags could ultimately lead to individuals' behavior in the physical world being tracked and integrated into profiles of their online activity.

Market Failures

Modern privacy and data protection regulation has two main economic objectives. The first is to ensure that national rules to protect individual privacy do not become a barrier to international trade by blocking the flow of personal data necessary for transactions and the provision of goods and services. The 1980 OECD guidelines were adopted at a point when half of its member countries had passed privacy laws. These guidelines are not binding on OECD members but have been significant in shaping privacy laws.

The OECD's expert group cooperated closely with the Council of Europe, which during the same period was producing a convention (CETS No. 108). The 1981 convention similarly includes an article that limits restrictions on personal data flows among signatories. It is open to nonmembers of the Council of Europe for ratification, and since 2008 a consultative committee has assessed accession requests from non-European states. Uruguay was the first to go through this procedure, and was invited to accede in 2011. In the medium term, the convention is the only realistic prospect for a global privacy instrument (Greenleaf 2013).

The most significant regional privacy agreement is the EU's Data Protection Directive (95/46/EC), which was developed under single-market procedures. The dual objective of the directive is to protect individual privacy while preventing the restriction of the free flow of personal data among member states. It implements the OECD Guidelines and Council of Europe

Convention, with additional protections including limits on data exports outside the EU and enforcement mechanisms—with a requirement for independent data protection authorities and individual rights of appeal to the courts (Greenleaf 2013). These additions were themselves introduced by the Council of Europe to strengthen the convention by its 2001 Additional Protocol (CETS No.181). In 2012 the EU began a revision of the directive and proposed a new directive to cover criminal justice agencies' processing of personal data.

The second economic objective of recent data protection rules is to protect consumer confidence in e-commerce, given the large quantities of personal data often gathered by online service providers. Numerous surveys have found significant individual resistance to online transactions due to concerns about giving away personal data and potential identity fraud.

Effective data protection has therefore been a key part of the European Commission's programs to encourage online consumer transactions, such as the Safer Internet Action Plan (Edwards 2004). This includes providing clear information to customers about how personal data are gathered and used, and more recently in some U.S. states and the EU, notification of breaches of data security to regulators and affected individuals (through the updated Privacy Directive 2002/58/EC as amended in Directive 2009/140/EC).

Both of these elements are stressed in the European Commission's plans for updating the data protection framework (2010). The commission vice president for the digital agenda, Neelie Kroes, told an industry roundtable that "users should feel they have the effective possibility to choose whether they want to be tracked and profiled or not. Irrespective of their legality, any such practices are damaging—they damage the already fragile confidence in the online digital economy. Today only 12% of Europeans fully trust online transactions, so this sort of behaviour is a case of the industry "shooting itself in the foot" (Kroes, 2010).

Fundamental Rights

The idea of protection of an individual's private sphere from government activity goes back to Aristotle (Westin 1967). It has been read into the U.S. Constitution by the Supreme Court and explicitly included in constitutions and treaties around the world. Privacy protection is a key part of the Universal Declaration of Human Rights, the International Convention on

Civil and Political Rights, and, more recently, the EU Charter of Fundamental Rights.

The U.N. Human Rights Committee has stated that the International Convention on Civil and Political Rights requires protection against interference in privacy by both state and private bodies, and regulation of "the gathering and holding of personal information on computers, databanks and other devices" (U.N. Human Rights Committee, 1988). The Council of Europe's Convention is the main international instrument implementing this more technology-specific focus on privacy, often referred to as "data protection." Alongside a general right to privacy, the EU Charter gives a specific right to data protection, which includes rights such as individual access to personal data.

Privacy is viewed as both a key individual, liberal right (especially in the United States) and a wider social good. It is seen to help secure individuality, autonomy, dignity, emotional release, self-evaluation, and positive emotional relationships. In Germany and some other countries, it is further seen to protect democratic rights to participation in public life (Bygrave 2010). Australian civil society groups captured these ideas in their Australian Privacy Charter (Australian Privacy Charter Council 1994), which states:

> A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organisations to intrude on that autonomy.
>
> Privacy is a value which underpins human dignity and other key values such as freedom of association and freedom of speech.

The protection of young people's privacy has particularly widespread support. This is because children are seen to be less able to make their own informed decisions about disclosing personal information than adults, and are at greater risk of harm from activities such as deceptive marketing or physical attack.

Article 16 of the 1989 U.N. Convention on the Rights of the Child protects against "arbitrary or unlawful interference" with children's "privacy, family, home or correspondence." Even the U.S. Congress, which generally takes a self-regulatory approach to private sector data protection, passed in 1998 the Children's Online Privacy Protection Act (15 U.S.C. sec. 6501–6506) with fair information practice requirements for Web sites targeted at children under thirteen years old.

Table 3.1
Public policy and market failure

Social impact of technology	Bandwidth, storage, processing capacity all doubling every 12 to 24 months, making it much easier for organizations to process and share personal data. E-government drives for personalization and savings; law enforcement and intelligence agency surveillance a further impetus.
Policy drivers—barriers to entry, network and scale effects, competition	EU promotion of a single market in data flows, personal data hoarding by information giants.
Fundamental rights in policy design	European Convention on Human Rights and EU Charter of Fundamental Rights key policy drivers.
Lesson	Privacy is a key human right that may need significant government intervention to protect.

Table 3.1 summarizes the public policy concerns and drivers relating to online privacy. This case study represents the clearest case of a fundamental rights concern leading to significant regulatory intervention in digital markets, led by European legislators and data protection regulators.

Types of Code Regulation

Online privacy protection in most jurisdictions has depended so far mainly on a notice-and-consent model, where users are informed of Web site practices related to the collection and processing of their data. Users are taken to consent to complex, legalistic privacy policies that are often dozens of pages long. In the United States, there is minimal oversight of this system by the FTC, which has complained that "current privacy policies force consumers to bear too much burden in protecting their privacy" (FTC 2010b).

Browser vendors tried to reduce this burden through the development of a platform for privacy preferences (P3P) standard. It allows Web sites to describe their data collection and processing practices in machine-readable format. In theory, it allows users to configure their Web browsers to only provide personal data to sites with privacy policies acceptable to that user. In practice, it had little impact. This was partly due to the complexity for small businesses of converting their day-to-day privacy practices into P3P terms and the difficulty in designing a usable browser interface that allows

users to easily understand P3P settings. There have also been significant concerns from privacy advocates that P3P would be unenforceable and pushed by industry as a replacement for rather than complement to data protection laws (Electronic Privacy Information Center 2000).

Aside from Microsoft Internet Explorer, P3P has only limited support in other browser software. The World Wide Web Consortium members could not reach consensus on a second version of the standard, and its development was suspended in 2007.

Further legal constraints apply in the EU under the Data Protection Directive and e-Privacy Directive. Personal data can be collected only for particular, specified purposes; not be excessive for those purposes; and must be deleted after use. Individuals have the right to access and correct personal data held by organizations.

EU states (and other jurisdictions with similar laws, such as Canada, Australia and Hong Kong) have independent national data protection regulators to oversee enforcement of these rights. The EU model has been extremely influential, seemingly initiating a race to the top in privacy regulatory standards, because it limits exports of personal data to countries without adequate standards of protection (Greenleaf 2013).

There is increasing evidence from behavioral economics that a "consent" model has significant failings. Very few users have the time or legal training to fully read and understand privacy policies, let alone enforce them. Privacy-related decisions are heavily context specific, dependent, for example, on how much a user is thinking about privacy at the time, along with his or her trust in the other party and often-inaccurate assumptions about how data will be used. It is extremely difficult to calculate the probability of harm that results from a single disclosure, let alone the cumulative impact, and what data could reveal when combined with a large number of other possible data sources.

This is illustrated by the U.S. situation, which in the private sector largely relies on individual action to recover damages suffered through a limited number of statutory rights. Courts are reluctant to award damages for data privacy offenses in the absence of monetary harm, and the cost of litigation is then disproportionate (Reidenberg 2006). Alternatively, the FTC has discretion regarding the pursuit of an action against a private enterprise. The FTC pursues only a small fraction of violations each year (Marcus et al. 2007). From 2002 to 2007, it brought only eleven actions for impermissible collection of personal information on the Internet from

children (FTC 2007). The action against the social networking site Xanga.com for illegally collecting information from 1.7 million children resulted in a fine of $1 million (less than $0.60 per child victim).

Organizations will adequately invest in protection of personal data only if they suffer the full costs to individuals of breaches of that protection. Limited enforcement to date of penalties for breaches is one reason for continuing successful attacks of the scale of that on Sony's PlayStation and Online Entertainment networks in 2011, where details were stolen from 102 million user accounts (Arthur 2011b).

Policymakers have therefore become concerned with increasing effective privacy protection for citizens, to protect individual autonomy and consumer interests, along with the wider democratic interest in a confident and powerful citizenry willing to engage in the public sphere (Bygrave 2010). Both the EU and the FTC are now looking to code solutions that will strengthen user choice over online tracking and embed privacy by design much more strongly into information systems within companies and government agencies that are processing large quantities of personal data.

Basic requirements for organizations to take technical steps to protect personal data were present in the 1974 U.S. Privacy Act and included as Principle 11 of the 1980 OECD guidelines: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data." Article 17 of the EU's Data Protection Directive similarly includes an obligation for data controllers to "implement appropriate technical and organizational measures to protect personal data." South Korean and Hong Kong law both provide more detailed security standards (Greenleaf 2011).

In practice, these provisions have had limited impact. Even European data protection authorities, who are much more interventionist than the FTC, rarely take steps to enforce this obligation. The only standards with significant deployment are the Payment Card Industry Data Security Standard, a self-regulatory framework covering companies that accept and process card payments. In some countries (including the United Kingdom), financial regulators have taken much stronger enforcement action than is available to data protection authorities against banks that have lost sensitive customer information.

The European Network and Information Security Agency (ENISA) has suggested regulators require the use of best available techniques, a process

already in use in European environmental regulation. For different application areas, regulators identify a "particular combination of technologies, protocols, standards, [and] practices" that should be used by data controllers (ENISA 2008, 35–36). An example of such standards is the series produced by Germany's Federal Office for Information Security, which covers the use of RFID tags in public transport e-ticketing, event ticketing, trade logistics, and employee electronic ID cards (Bundesamt für Sicherheit in der Informationstechnik 2010).

Behavioral Advertising

In the online world, behavioral advertising, with its widespread profiling of user browsing, has become an increasingly common practice. In 2011 advertising company WPP announced it had built profiles on over 500 million users in North America, Europe, and Australia. Policymakers in the United States and EU have responded with more specific regulation targeted at the browser software functionality that enables this profiling.

The EU's e-privacy directive, updated in 2009, requires consent from users before the "storing or accessing of information stored in the user's terminal," mainly targeted at the "cookies" that Web sites commonly use to track user activity. Users must be given "clear and comprehensive" information about how their data will be used and can give consent using browser options as long as that is "technically possible and effective."

Browsers that accept cookies by default do not meet this test, according to the European Data Protection Supervisor (EDPS), since most users lack the skills to change these settings. The EDPS suggests instead that browser software provide a more user-friendly "privacy wizard" or other user interface to help users decide whether they wish to be tracked and receive targeted advertising, with the default setting that they do not (Hustinx 2011).

The FTC has focused on a related mechanism: a "persistent browser setting" that can be used to signal that a user does not wish to be tracked by third parties or served targeted advertisements (FTC 2011). This "do-not-track" option has quickly been added to browsers such as Firefox and praised by U.S. and EU politicians—with U.S. president Barack Obama launching a "consumer privacy bill of rights" that encourages companies to implement such measures and asking Congress to give them statutory backing (U.S. Government 2012). The EDPS has added that a do-not-track

standard would be one way for advertisers to comply with the e-privacy directive, so long as the default setting was privacy protective (EDPS 2011b).

Although industry associations have promoted self-regulation for behavioral advertising, examples such as Google's circumvention of privacy controls in Apple's Safari browser (Mayer 2012) have increased pressure for regulatory intervention.

Privacy by Design

The EU and FTC have broadened these regulatory proposals to other technical systems that process personal data. By focusing on privacy protection right through the technology life cycle, regulators have called for privacy to be embedded by design into new systems (U.K. Data Protection Registrar 1999; Cavoukian 2009). Requiring this principle to be followed is a key aim of the revision of the EU Data Protection Directive (European Commission COM(2010) 609), with Commissioner Viviane Reding telling the European Parliament that "Privacy by Design will lead to better protection for individuals, as well as to trust and confidence in new services and products that will in turn have a positive impact on the economy" (Reding 2010). The FTC has similarly proposed that "companies should adopt a 'privacy by design' approach by building privacy protections into their everyday business practices" (FTC, 2010b, v).

One mechanism that companies can use to signal such an approach is to gain certification from independent auditors. The most in-depth assessment tool is the EuroPRISE seal developed by the data protection agency of the northern German state Schleswig-Holstein. Approved assessors examine the software and development processes behind information technology products and services, ensuring that they include privacy-protective functionality throughout. German public procurement rules allow government agencies to give preference to such certified products (Korff and Brown 2010).

Internet of Things

The Internet of things is the second area where privacy regulators have taken specific steps to shape the development of technology to better protect personal data, beginning with RFID tags. The industry association GS1 estimated that around 87 billion tags would be deployed in Europe between 2010 and 2020 (GS1 and Logica 2007), and there has been

understandable public interest in a technology that some privacy campaigners have characterized as "spy chips."

In response, the European Commission has recommended that industry should develop a framework for privacy assessments of RFID applications, "in collaboration with relevant civil society" and subject to approval by the data protection authorities of the EU member states (C (2009) 3200). The second proposed version of the framework was approved in 2011. It is designed to help operators of RFID systems to "uncover the privacy risks associated with an RFID Application, assess their likelihood, and document the steps taken to address those risks" (Article 29 Working Party 2011a, Annex A3). It covers the tags themselves, as well as "back-end systems and networked communication infrastructures" used to process tag data.

The framework encourages the creation of industry and application-specific templates. It includes an initial analysis step, followed by a small-scale or full-scale risk assessment phase. The application operator then describes the technical and organizational steps taken to mitigate these risks in a Privacy Impact Assessment Report, which should be available on request to national regulators. The report must also include a detailed inventory of data items stored and processed and a list of internal and external data recipients.

While the risk assessment process is focused on the Data Protection Directive principles, the framework can be easily adapted for use in other jurisdictions and had significant input from non-European companies. This format means that a PIA can also be used to carry out a legal compliance check for a system; companies are unsurprisingly reluctant to carry out a separate PIA and compliance check (Spiekerman 2011).

Table 3.2 summarizes the features of code regulation now being explored by regulators, particularly within the EU, in an effort to improve the

Table 3.2
Types of code and code regulation

Layer	New focus on RFIDs, browser code (do not track, cookies) and privacy by design.
Location (manufacturers, ISPs, servers, clients)	Software and system architects.
Enforcement of code	Threat of Data Protection Directive enforcement; revision of Data Protection Directive to include more specific requirements for privacy by design.

efficacy of privacy protection—initially in the Internet of things and with behavioral targeting for adverts.

Institutional Political Economy

In Europe, where privacy has long been seen as a core requirement for democratic government, legislators and statutory regulators have played key roles in promoting and enforcing privacy regulations. They have been strongly supported by national constitutional courts and the European Court of Human Rights, which has made technology-specific decisions such as requiring better security protection for large databases of personal information (*I* v. *Finland*, 2008) and stopping states from building large databases of sensitive forensic information from unconvicted individuals (*S and Marper* v. *UK*, 2008).

The European Parliament has played an increasingly significant role: a leaked U.S. State Department cable noted that "the media-savvy EP has cultivated a high profile role on data protection policy through public hearings, resolutions, non-binding statements, opinions, and lobbying the Council and Commission for action" (U.S. Mission to the EU 2009).

States with a particularly strong constitutional tradition of privacy protection, such as Germany and Austria, have played a significant role in the development of EU data protection law. The German Constitutional Court's notion of informational self-determination, developed in its 1983 decision on the national census, has influenced later legislation and judicial decisions across the continent, and led to the inclusion of specific rights to privacy and data protection in articles 7 and 8 of the EU Charter of Fundamental Rights. These will play a key role in decisions of the European Court of Justice on issues such as the mandatory retention of personal data by ISPs and telephone companies under the Data Retention Directive (Directive 2006/24/EC).

The EU has successfully influenced other regional privacy laws by restricting the transfer of personal data from member states to countries without adequate privacy protection. This determination of "adequacy," overseen by the European Commission, in practice requires other states to introduce most of the key protections from the Data Protection Directive into their own national laws.

The commission has now assessed Argentina, Canada, Israel, New Zealand, Switzerland, Uruguay, and five smaller European territories to meet this test. Greenleaf (2013) argues that Colombia, Mexico, Peru, South Korea, India, Taiwan, Hong Kong, and Australia could all put up a case that they could meet the adequacy test, as could some western African states.

Against these European governmental and judicial advocates for stronger privacy protection, resistance has come particularly from the U.S. government, where politicians have been strongly lobbied by technology and services companies and national security agencies that want greater access to personal data. U.S. policy goals were succinctly summarized by the mission to the EU: "to ensure that data privacy rules will not hinder economic growth, endanger economic recovery, or discourage greater [law enforcement] cooperation" (2009). The U.S. Supreme Court has at times protected privacy against the state under the Fourth Amendment to the Constitution (*Katz* v. *United States,* 1967), but has also found some privacy rules to conflict with the free speech guarantee in the First Amendment (*Sorrell* v. *IMS Health,* 2011).

The United States has tried to influence international privacy regulations by leading a policy development process in the Asia-Pacific Economic Cooperation group, intended to supplant stronger European standards. This process has focused on accountability for harms caused by privacy breaches rather than detailed rules on data handling. It has so far had limited success. Many members of the Asia-Pacific group have since found it in their own interests to base new laws on the EU Data Protection Directive. Analyzing these efforts, Greenleaf (forthcoming) concluded that "attempts by US companies and the US government to use their combined economic and political influence to limit development of data privacy laws in other countries will continue to be important, but are probably now on the wrong side of history."

Significant opposition to privacy rules has also come from a wide range of law enforcement and intelligence agencies. The terrorist attacks on the United States in September 2001, on Madrid in 2004, and on London in 2005 all gave significant impetus to counterterrorism agency demands for access to more personal data. While many countries' privacy regulations do not apply to data processing for these purposes, security agencies increasingly trawl through commercial databases that are subject to data protection rules.

Former U.K. security and intelligence coordinator Sir David Omand (2009) wrote that intelligence agencies would need blanket access to "personal information about individual [sic] that resides in databases. . . . Access to such information, and in some cases the ability to apply data mining and pattern recognition software to databases, might well be the key to effective pre-emption in future terrorist cases" (9).

In the EU, the blanket exemption of Justice and Home Affairs policy from the directive ended when the Lisbon Treaty came into force in 2010, with this policy area becoming the joint responsibility of member states and the European Parliament. The U.S. administration faced significant opposition from the parliament during the drafting of U.S.-EU treaties that would provide U.S. access to European passenger name records (related to air travel) and Society for Worldwide Interbank Financial Telecommunication payment records (de Hert and Papakonstaninou 2010). The U.S. Mission to the EU strongly criticized the European Commission for a failure of policy leadership, allowing the EDPS and national data protection authorities to "regularly make high-profile public statements on areas outside of their formal competence . . . [which] tend to give primacy to civil liberties-based approaches for the EU's Single Market, consumers, or law enforcement" (U.S. Mission to the EU 2009).

Advocacy groups have played an important role in campaigning for stronger privacy laws, highlighting actual and potential abuses by governments and companies and bringing test cases before courts and regulators. Their strategies have included influencing media and political discourse; conducting research and providing information to the public and politicians about the privacy consequences of policy proposals (often making heavy use of freedom of information laws); and "naming and shaming" organizations (Bennett 2008). This includes participating at the annual international conference of privacy regulators, open to anyone who can afford the (not insignificant) conference travel and registration costs, for which some funding has been provided by philanthropists such as George Soros' Open Society Foundations.

Privacy is of interest to many Internet users around the world, and privacy advocates have made extensive use of the Internet to share information and coordinate their campaigns. They have also built issue-specific coalitions around issues such as behavioral advertising and RFID tags. These activism networks are open and easily reconfigured, facilitating fast-paced campaigns against invasive new policies or products. This quality

may, however, make it more difficult for campaigns to achieve longer-term goals and growth. As Bennett concluded, "There is clearly no worldwide privacy movement that has anything like the scale, resources, or public recognition of organizations in the environmental, feminist or human rights fields" (Bennett 2008, xv).

Regulators and civil society have had some success in persuading software companies to improve the privacy protection in their products. There has been occasional competition on privacy functionality between search engines (Bing, Google, and Yahoo!) and browser vendors (Mozilla, Microsoft, and Apple). Mozilla was praised by the FTC and European Commission after introducing a do-not-track option in its Firefox browser. However, these companies often face conflicts of interest, particularly where they derive revenue from advertising. For example, Microsoft made an improved "private browsing" mode harder to leave switched on in Internet Explorer after pressure from the advertising division of the company (Soghoian 2011).

Internet advertising companies have lobbied heavily against "unnecessary and ill-informed" EU rules on targeted advertising. Their industry association, the Internet Advertising Bureau Europe, lobbied unsuccessfully against the creation of sector-specific rules on data protection for electronic communication services in what became the 2002 e-Privacy Directive. The European Parliament amended the draft directive to include a specific ban on the use of cookies without explicit user consent, but these were modified during negotiation with the commission and council to allow an opt-out approach. This was the result of an industry Save the Cookies campaign that emphasized the costs and competitiveness impact on European companies. Privacy advocates had placed a higher priority on protecting the rules in the directive banning unsolicited e-mail (Kierkegaard 2005). However, privacy regulators and advocates reversed this opt-out provision at the next revision of the directive in 2009. The industry has continued to push a self-regulatory model, producing a Best Practice Recommendation on Online Behavioral Advertising (European Advertising Standards Alliance 2011).

RFID standards have developed more slowly, partly because computing hardware evolves less quickly than software. Little consideration was given to privacy in the original RFID standards. This changed when advocacy groups began campaigns against what they called "spy chips," something

that resonated strongly with voters and led to pressure from policymakers and politicians (Bennett and Raab 2006).

The European Commission's approach was to set up an informal RFID working group of industry, academic, and civil society representatives to agree on a coregulatory framework code. The industry representatives were initially reluctant participants, producing a "barely structured pamphlet" lacking any risk identification process or link to European privacy laws. Civil society had little input into this document and felt their presence at working group meetings was being used to legitimate a document being written largely by the GS1 trade association (Spiekerman 2011).

Unsurprisingly, the Article 29 working party of data protection authorities, whose approval was required by the European Commission, rejected this proposal. An alternative industry consortium produced a much stronger second code with academic input and threatened to submit this code for approval. This pressure led to industry agreement within the working group with civil society on a compromise code, the third effort, which was finally approved by the Article 29 working party (2011c).

Table 3.3 summarizes the institutional policy economy of online privacy protection. It makes clear that national data protection agencies and, to a lesser extent, consumer protection agencies play a clear role, with some significant opposition from industry actors with a commercial interest in greater processing of personal data. The extremely effective alliance described in the next chapter between Internet users and industry over proposed copyright measures would be less likely to arise in a privacy context.

Outcomes

It can be difficult to assess the impact of privacy and data protection regulation. Strong laws and enforcement agencies can be less important in practice than the degree to which government attitudes, industry standards, and cultural factors are supportive of privacy. Data protection agencies often prefer to work through private negotiations with government and industry rather than through high-profile enforcement actions. Privacy rules aim to prevent abuses before they occur (Bygrave 2010). The privacy impact of public and private sector actions can vary across different sections of society (Bennett and Raab 2006).

Table 3.3
Institutional political economy

Key actors: national, regional, global	National data protection regulators; consumer protection agencies (e.g., FTC). Coordination in EU, Council of Europe, Asia-Pacific Economic Cooperation. Law, enforcement agencies, advertisers, and their technology partners.
How legitimate and accountable?	Regulators are mainly legislative creatures and hence democratically accountable, although self-regulatory policy outside the EU is less legitimate or accountable.
Multistakeholderism	Annual regulators' conference open to all stakeholders. RFID process explicitly multistakeholder, although industry tried hard to ignore civil society.
Key technical actor buy-in	Firefox (Do Not Track), Apple Safari blocks third-party cookies by default (no ad network, unlike Microsoft and Google). RFID industry wrote privacy framework with some other stakeholder input; code approved by Article 29 Working Party.
Lessons	Strong intervention from legislators and privacy regulators is sometimes needed to counteract the powerful voice of law enforcement agencies and technology companies that have shared interests in weaker restrictions on access to personal data.

That said, there is widespread recognition of the EU's detailed rules as a gold standard to which many other jurisdictions aspire (Greenleaf forthcoming). The European Commission is strengthening and broadening these rules during the revision of the data protection directive, especially regarding incentives for privacy by design.

At the other end of the scale, there is clearly less protection for individual privacy in the U.S. legal system than in most other advanced economies. Outside the federal government, regulation is patchy, sector specific, and state-by-state, with limited individual rights and enforcement only under very specific circumstances by the FTC (Hoofnagle 2010). Most responsibility is placed on consumers, regardless of their capability to understand legalistic privacy notices or the availability of other options in often concentrated markets.

This is problematic, given the geographic (and cultural) location of most major Internet companies' headquarters. Many U.S. companies emphasize the need for consumer "empowerment" and dismiss European-style rules as bureaucratic, ineffective, and obstructive of innovation.

Consumer education and action are important parts of any data protection regime, and one study found that U.S. consumer Web sites had privacy policies at least equivalent to, and in some cases better than, EU sites (Scribbins 2001). But notice-and-consent and self-regulatory regimes have not in general proved effective in the face of government and industry interest in access to ever-greater quantities of personal data. They work best as elements of a broader, statutory regime (Greenleaf 2013).

This is not to say the EU has reached privacy nirvana. Several studies have found that data protection authorities are underresourced; that companies generally support privacy rules, but have a mixed record in following them; and that individuals have a limited awareness of their rights (Bygrave 2010). Greenleaf (2013) speculated that "many businesses and government agencies internalise the norms of data privacy principles once they are enacted and observe legislation to a significant extent even in the absence of effective enforcement activities."

The OECD guidelines requiring data controllers to take "reasonable security safeguards," echoed in the data protection directive's "appropriate technical and organizational measures to protect personal data," have not been enough to stop some spectacular breaches of large databases, such as Sony's loss of 102 million users' PlayStation and Online Entertainment account data (Arthur 2011b). Given the widespread availability of encryption tools to prevent unauthorized data access, it is extremely surprising that many of these breaches were technically trivial. The lack of enforcement of minimum standards is one reason for this.

As legal requirements have spread in U.S. states for organizations to notify customers of breaches (Hoofnagle 2010), there is a greater risk for careless organizations of reputational damage and claims for individual losses, although these can be difficult to quantify (Acquisti, Friedman, and Telang 2006). Studies have shown little long-term impact on the share price of companies affected by data breaches (Acquisti, Friedman, and Telang 2006). Privacy harms are frequently probabilistic and long term, making it difficult for courts to assess damages (Acquisti 2002). But outcomes in the United States have been persuasive enough for the European Commission to add breach notification during the revision of the electronic communications framework, and to other information society services in the revision of the data protection directive.

There has been significant research into privacy-enhancing technologies (PETs) that could provide much stronger technical protection of personal data, but very little mainstream deployment of these tools. One explanation, despite "relatively high levels of concern about privacy in online settings," is "widespread indifference on the part of individuals when it comes to actual buying decisions. . . . Market imperfections, which can include asymmetric information, externalities, lack of information sharing about privacy risks and coordination failures, mean that the individually rational decisions of data controllers do not necessarily lead to the optimal level of PETs deployment" (London Economics 2010, xi). Another is that adoption requires a certain critical mass of users that has not yet been reached and may require support from data protection authorities and public bodies. Many businesses do not yet fully understand the costs and benefits of PETs and so have delayed their deployment. But this leaves customers with little meaningful choice over whether to disclose personal information (London Economics 2010).

There can also be significant opportunity costs in adopting PETs. Many organizations use personal data to supply targeted advertising, offer personalized services, or adjust prices based on a customer's previous willingness to pay. They will accept the loss of some of these benefits by deploying PETS only if there are at least equivalent gains from attracting privacy-sensitive customers, avoiding potential reputational damage, or meeting regulatory requirements (Rubinstein 2012).

Regulators in the United States, Canada, and the EU have recently focused on code in browsers (for behavioral advertising and social networking) and RFID systems. While some regulators have been calling for the use of privacy-by-design principles since the 1990s, it has taken the threat of enforcement action to persuade some companies to take these principles seriously. Most notably, the federal Canadian privacy commissioner took action in 2009 against Facebook over its photo-sharing and "app" Web site features and persuaded the company to introduce more privacy-friendly default settings (Smith 2009).

Without such action, industry self-regulatory efforts have generally been weak and rejected as such by civil society. For example, the World Privacy Forum (2011) criticized the draft European Advertising Standards Alliance code on behavioral advertising as "dismiss[ing] consumer privacy concerns by not engaging with them in any significant way" (2011, 2).

The second version of the code more strongly emphasized its complementarity to consumers' legal rights under the e-privacy directive, but was still found by the Article 29 Working Party to be "not adequate to ensure compliance with the current applicable European data protection legal framework" (2011b). As Winn (2010) observed: "The institutional differences between European and US standards systems is due in part to the greater deference of US regulators to market-oriented private-sector standards bodies. . . . If EU regulators decide they want to integrate ICT standards into the existing framework of EU data protections laws, then they may have no choice but to find a way to out-maneuver US efforts to minimize government intervention in global information networks." That said, the FTC and Obama administration have gone further than expected in promoting privacy in technical standards.

It is too early to judge the impact of the privacy-by-design regimes being introduced by the European Commission and elsewhere. Detailed technology-specific rules can become outdated very quickly and risk constraining innovation without preventing invasions of privacy through different technologies. The online advertising industry has criticized the cookie provisions of the e-privacy directive in these terms, although regulators have responded that they are essential to give users control of behaviorally targeted advertisements.

Rubinstein (2012) suggests several measures that the FTC could adopt to support privacy by design were Congress to give them such powers in new privacy legislation. These include allowing organizations to experiment with new approaches to achieve privacy goals, such as standardized, easy-to-read privacy notices, in exchange for exemption from detailed regulatory requirements. Such approaches could be part of more general safe harbors that provide industry sectors with flexibility in their approach to meeting statutory requirements and were echoed in the Obama administration's plans for enforceable consumer privacy rights (U.S. Government 2012).

The EU RFID privacy framework could prove to be more widely influential in terms of privacy regulation. Rubinstein suggested the FTC use a similar process of negotiated rulemaking to bring together industry, civil society, and regulators to agree on behavioral advertising rules (2012, 32). Senior European Commission officials have stated that they hope the RFID framework will be a model for initiatives in other areas, such as

Table 3.4
Outcomes and divergences

Transparency	Limited impact of opaque privacy policies and user education, which are often unintelligible to users, who often are in a poor position to judge privacy risks.
Enforcement	Varied levels of enforcement by EU regulators suggest cultural factors also important.
	Data breach requirements and code solutions could increase privacy protection more uniformly.
Interoperability	Broad European standards are driving a global race-to-the-top, with export controls and "adequacy" assessments driving interoperability between national regimes.
Efficiency	Efficiency via internalized data controller self-enforcement? Norm enforced by law.

cloud computing and online advertising (Santucci 2011). They foresee several benefits over traditional data protection regulation. For example, action by RFID application operators can reduce the privacy compliance burden on small businesses that use turnkey systems with only minor customization.

The coregulatory process that led to the approval of the framework was fraught with obstacles (Spiekerman 2011) but ultimately succeeded in incorporating technical expertise from industry and academia while achieving privacy protection acceptable to the EU's data protection authorities. Time will tell whether the process has achieved sufficient industry buy-in to avoid the need for later enforcement action by regulators. In chapter 6 we assess the impact of similar coregulatory proposals on social networking sites.

Table 3.4 summarizes the outcomes of online privacy regulation, noting that the industry-preferred regulatory option of transparency and consumer choice has had limited success and that the greater market intervention of European regulators has had some impact even on the U.S.-dominated sector of behavioral advertising.