

The New Economy: Transatlantic Policy Comparison
Data Privacy
By
Abe Newman

A central concern of privacy is the ability of an individual to control the access to and use of personal information. New technologies, which radically enhance data production and processing, challenge privacy expectations. Societies around the world wrestle with the question over where the new lines of privacy should be drawn. On the one hand, numerous private and public sectors of the economy employ personal data as vital economic capital. Direct marketing, insurance, telecommunications, health care and welfare administration rely on data management to enhance efficiency and reduce costs. On the other hand, individuals and privacy advocates resist and protest the eclipse of privacy for the sake of economic efficiency. As uses of personal information clash with concerns over information autonomy, regulation mediates the debate. Much like welfare systems, which emerged in the wake of the industrial revolution, the regulation of personal data use will have far reaching implications for the development of industrial economies in the 21st century.

In the late 1960s and early 1970s, concerns arose over government proposals to centralize public data collection. Meant to assist social policy management and expansion, national government databases led to successful coalitions across industrialized countries for data protection regulation. This first wave of data protection policy concentrated on the formulation of basic principles that were intended to guide future data protection efforts. These principles have come to be known as the Fair Information Practice Principles (FIPP) and rest on the following concepts: Notice – data users should openly notify data subjects of privacy policies; Consent – data should not be disclosed or used for purposes without data subject consent; Security – stored data must be secure from theft or corruption; Access – data subjects should have access to stored data in order to verify validity; Accountability – a procedure must exist to enforce and punish breaches of the principles.

At the fore of the movement to enshrine basic privacy principles, the German State of Hessen passed the first comprehensive data privacy law in 1970, followed by the Swedish Privacy Act in 1973 and the German federal regulation in 1977. Europe has continued this leadership in privacy protection through the passage of the EU Data Privacy Directive in 1995. The U.S., in contrast, has rejected comprehensive government regulation, opting for limited sectoral policies and industry led initiatives. How do these systems differ across and within regions? How well suited are they to meet the challenges posed by new data collection technologies? What will the differences mean for the use of information in both the public and private sector? Do regulations vary in their relative efficacy concerning data privacy protection? How do existing protection systems forge new political interest and coalitions around future privacy concerns?

Propositions for Discussion

Proposition 1. Digital Challenges Ignite Privacy Debate: With the codification of the FIPP in international agreements like OECD guidelines on information use and the European Union Privacy Directive, the basic principles of data protection are internationally recognized. This general consensus, however, does not guide specific responses to new data collection technologies. The development of technologies like chip-cards, genetic testing, e-medical records, and location monitoring redefine personal information collection possibilities. The power of these technologies to monitor individual behavior raises new calls for regulation. The next round of battles is not about whether data protection should occur or over the basic policy principles of data privacy. Battles will instead concern the implementation of FIPP to specific applications of digital technologies.

Disputes over the appropriate use of certain data collection technologies pits economic interests against individual information autonomy. The opt-in consent requirements for healthcare as opposed to opt-out for finance in the U.S. exemplifies this trend. Differences in industry and government interests like those of doctor associations, financial service providers, insurance companies, direct marketers, and advertising agencies will produce variation in acceptable personal data use across national economies. New coalitions emerge that pit those benefiting from information monitoring against those that lose decision-making freedom.

Proposition 2. Regulatory Variation Persists: Enforcement of the FIPP and specific responses to new technologies differ across countries. Although the EU Directive succeeded in preventing escalating trade tensions among member states, the character of the directive allows for considerable variation in national implementation. Instead of unifying on one common mechanism of enforcement, multiple distinct institutional designs continue to exist within the EU. The centralized French monitoring organization concentrates on databank licensing while the decentralized network of German regulators work to advise legislators and private sector actors. The French system's focus on licensing becomes increasingly taxing as the number of organizations with databases rises. This focus drains resources, hampering the organizations' ability to respond to consumer complaints and enforce audits. The federal structure of the German system spreads out regulators. The layers of privacy authorities provide advice and support for private sector actors wishing to comply with data protection legislation or create self-regulatory solutions.

Outside of Europe a variety of responses exist. In Japan, MITI coordinates seal programs. The United States relies on publicity and pressure from NGOs and enforcement by the FTC to protect privacy interests. Are some data protection institutions better equipped to confront digital challenges? Do different data protection systems provide certain states an institutional comparative advantage in data privacy protection?

Proposition 2. Effective Data Protection is a Thing of the Future: Data protection relies on three basic implementation mechanisms: government, business, and technology. The first wave of privacy policies focused on the potential government abuse of

databanks and relied on government regulation as the central means of control. As the primary threat to data privacy shifts from the government to businesses what mix of the three strategies might produce adequate protection at a minimal cost?

Technological responses will no doubt play an integral role in the new architecture of control. Microprocessors are embedded in more and more products and linked to expanding numbers of communications networks, increasing data collection points and linkages between data users. As physical choke points for regulation disappear, governments and businesses will rely on technological controls to reduce unwanted privacy abuses.

This does not mean, however that technology alone resolves privacy dilemmas. Legislation will be used to enforce computer code just as computer code will be used to reinforce legislation. Political interests and institutions will influence national decisions regarding technological controls. The role of governments and business will differ cross-nationally. European governments encourage standardization around common technological solutions like the Platform for Privacy Preferences (P3P) while different groups like TRUSTe, Zero-Knowledge and Zoom compete in a North American market for technological responses. How does variation in data protection regulation affect the adoption rate and character of privacy enhancing technologies (PETs)? Does the centralized European system hamper flexible solutions? or does the U.S. system lack the capacity to monitor industry brokered deals?

Background for Discussion

In the mid1960s, government agencies were some of the few organizations capable of purchasing supercomputers powerful enough to sort and analyze large quantities of data. As states expanded social programs and services, governments looked to use the technical capacity of centralized data processing to augment bureaucratic control. These efficiency gains, though, aroused equally powerful surveillance paranoia. Coalitions formed to support legislation intended to check government abuse of new data processing technologies.

This first wave of regulation focused on the creation of general principles and implementation mechanisms. These laws date back to the Swedish Data Privacy Act of 1973 or the U.S. Privacy Act of 1974 and were internationally codified by the OECD in the 1981 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. These principles have become known as the Fair Information Practice

Principles (FIPP).¹ The European Union Data Privacy Directive adopted in 1995 completes this wave of comprehensive regulation. The Directive requires member states to adopt comprehensive data protection legislation following the Fair Information Practice Principles (FIPP) and establish an independent national data protection commission.

Information technology innovations raise additional privacy concerns and potentially strain the capabilities of these first regulatory efforts. Aside from debates concerning the response to the September 2001 terrorist attacks, the primary agent of privacy intrusion has shifted from government actors to the private sector. Initial privacy laws passed during the 1970s focused their attention on public sector threats. The Orwellian vision of Big Brother depicted in *1984* was long heralded as the ultimate justification for privacy protection. But information technology empowers private actors as much as public officials. Distributed networks and personal computers provide average businesses with data processing capacities previously reserved to the largest corporations and public agencies. Additionally, deregulation and fiscal constraints increasingly force public bureaucracies to rely on private sector information sources. The threat of personal information abuse transforms from a government based surveillance society into something better described by an AOLianworld where consumer monitoring expands at rapid speeds.

Additionally, new data collection technologies augment monitoring capacities. First, the quantity of information that one can accumulate and analyze is increasing

¹ The principles include: Notice – data users should openly notify data subjects of privacy policies; Consent – data should not be disclosed or used for purposes without data subject consent; Security – stored data must be secure from theft or corruption; Access – data subjects should have access to stored data in order to verify validity; Accountability – a procedure must exist to enforce and punish breaches of the principles.

exponentially. Web trails, credit card records, and club cards generate growing amounts of personal data. With the rise of data banks and data processing programs, staggering amounts of information can be stored and dissected into refined profiles of individual behavior. Second, the rise in information gathering changes the quality of collected information. As the capacity of data monitoring improves, new areas of human behavior fall under public scrutiny.

This rise in the quantity and the quality of personal information collection and use alters the character of privacy expectations. The U.S. as well as many European nations base privacy protection on the assumption of a “reasonable expectation of privacy”. It is not the data itself that is protected but the use of the data in a particular context. For example, an individual might want a doctor to know that they have a disease but not want an employer to have the same information. Privacy rights protect a particular use of information and not the information itself. As information technology challenges preexisting public and private boundaries, conflicts emerge over appropriate levels of privacy for specific digital technologies.

Digital Challenges Ignite Privacy Debate: Public concern over private sector

collection, storage, and analysis of commercially produced information grew over the last two decades, threatening the future commercialization and spread of information driven innovations like e-commerce. The most recent wave of privacy legislation is addressing difficult questions centering on the acceptability of certain new monitoring and data collection technologies, for example the appropriate use of video technologies, location monitoring, e-medical records, and chip-cards.

These technologies have the capacity to redefine the current borders of the private sphere. If location monitoring became an accepted practice, marketing firms could track daily movements and then target individuals with certain products at specific locations. Similarly, the broad acceptance of video surveillance in the workplace and other public settings radically alters how individuals conceive of autonomous space.

As the push for specific sector or technology regulation emerges, political battles intensify and new coalitions for and against privacy emerge. As more and more industries use personal information to provide their services, information becomes valuable capital. Therefore, attempts to regulate specific personal data use or collection engenders the type of interest group conflict previously associated with traditional industrial lobbies. Coalitions emerge that pit those benefiting from information monitoring against those that lose decision-making freedom.

The 1997 EU Telecommunication Directive, 1999 Gramm-Leach-Bliley financial privacy rules, and the 2001 Medical Privacy Rules all typify the next round of data protection legislation. They are characteristic of the transition from broad legislation and sweeping principles to specific implementation procedures. Broad political consensus around the FIPP fades as concrete interests are threatened. The difference between opt-in and out requirements in the Medical Privacy Rules versus the financial privacy regulation serve as a case in point. Medical rules were developed and debated by the department of Health and Human Services after Congress delegated rule making authority in 1996 while the financial services rules were a byproduct of Congressional financial modernization legislation. Different policy-making processes permit different interest groups varying amounts of access in this new round of data privacy regulation.

Regional variation in interest group alignments influences the texture of the debates on either side of the Atlantic. The lack of data privacy protection for the Internet in the U.S. stems in part from the inherent tension between data protection and freedom of information. Interestingly, a set of electronic privacy advocates emerged in the early 1990s including groups like the Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation (E.F.F.). These digital freedom advocates receive minimal support from traditional civil liberty organizations like the ACLU. The ACLU sees data protection as a threat to free speech and therefore limits its involvement in data privacy issues. Although this tension plays a lesser role in Europe owing to less encompassing free speech rights, a different conflict exists. Consumer protection groups press for detailed accounts of consumer transactions and data protection officials call for data frugality. These and other differential interest group configurations will overlay emerging regulatory conversations concerning gene-testing, e-medical records, location monitoring, and direct marketing.

Regulatory Variation Persists: Despite convergence around the FIPP and the EU Privacy Directive, national regulatory variation continues to persist both within Europe and across major industrialized economies. Legacies from earlier data privacy efforts influence government responses. Looking at the three largest economic regions in the world, a diversity of regulatory patterns emerges.

Europe has comprehensive legal regulation of data privacy but there is diversity in the enforcement mechanisms adopted by different member states. The European Union Privacy directive required national enabling legislation which permits this variation.

European countries with existing data protection agencies relied on their specific strengths when adapting the directive to national settings. For example, the French monitoring agency, the CNIL, is a centralized agency that focuses its efforts on database licensing. Lacking the resources to audit large segments of the public sector, the agency is more involved in data use by large corporations or public sector initiatives. The German authority, in contrast, functions in a decentralized manner with layers of data protection agencies at the various tiers of government. Local data protection officials coordinate with regional businesses to develop data privacy policies. As a result, German agencies are better positioned to facilitate private sector solutions although they have fewer formal powers than the CNIL.

Lacking a centralized data protection authority from the first wave, a patchwork of regulators and NGOs respond to data privacy concerns in the U.S. Data privacy protection is organized around sectoral lines. Certain industries like health care and video rentals have clearly defined laws while other industries like data marketing face no specific regulation. At the center of the U.S. systems sits the FTC which reviews breaches of FIPPs. The U.S. regulatory system responds when companies break promises concerning data protection. NGOs monitor and draw attention to private sector missteps. This system of enforcement encourages companies to adopt preventative measures to reduce bad publicity. Firms also have an incentive to avoid sweeping privacy commitments that might open them up to suits based on unfair trade practices.

Japanese initiatives, unlike those in the U.S. and Europe, are not influenced by previous waves of data protection. Emerging as a response to the European Union Privacy Directive, Japanese data protection is coordinated by MITI and a number of

industry associations. Viewed primarily as a trade issue, as opposed to a domestic policy concern, MITI has taken the lead role in developing data protection standards. Mirroring U.S. responses, government policies encourage business efforts like seal programs and self-regulation. A recent agreement between TRUSTe and the Japanese Engineers Trade Association, gives TRUSTe jurisdiction to offer its seal program and dispute settlement mechanism to Japanese web sites.

Effective Data Protection is a Thing of the Future: The decentralization of information exchanges through networked technologies challenges the appropriateness of purely government mandated standards. Many command and control regulatory strategies seem almost farcical as data collection technology is embedded into more and more machines and then connected to an ever-increasing number of networked systems. As more and more entities have the capacity and resources to develop sophisticated data collection and processing systems, regulatory agencies find their resources strained. This problem is typified by the French, Swedish, and British agencies, all of which continue to view database registration as a primary data protection tool. They devote so much effort to registration that lose their ability to audit or follow up on consumer complaints.

The current regulatory difficulties do not imply, however, that digital networks will remain the free flowing, decentralized Internet of the mid 1990s. Public and private sector organizations have an incentive to impose some structure on data networks: Firms seek to increase knowledge extraction and governments hope to reclaim authority. In addition to government regulation, industry self-regulation and technology offer potential regulatory solutions.

Technology will no doubt play an integral role in the emerging system of regulation. Government mandates will be supplemented by and may encourage technological interventions that limit or channel data transmissions. Like one-way streets directing the flow of traffic, digital architectures may be imposed through computer code that serve to promote data protection legislation. The reverse will undoubtedly also occur. Legislation will enforce computer code as happened with the Digital Millennium Copyright Act.

Government data protection regimes influence the character of emerging technological solutions. For example, central data authorities in Europe coordinated their initial efforts at promoting privacy enhancing technology (PETs) for the Internet around the Platform for Privacy Preferences (P3P). Using European Union research monies and the bully pulpit of data protection authorities, the European Union has attempted to coordinate a standardized response to data protection concerns on the Web. The U.S., in contrast, lacks a centralized data protection authority to mediate such efforts. Instead, the threat of Federal Trade Commission investigation or negative press rallied by NGOs encourages companies to adopt a variety of PETs. A diverse group of firms like TRUSTe, Zero-Knowledge, Webwasher and Zoom compete in the North American market for technological responses to concerns over Internet privacy.

Conclusion: The combination of new privacy coalitions, government institutions, and technological controls shape the borders of privacy in a digital age. Variation in the three elements across countries will produce different political bargains over appropriate protection. The character of these solutions will affect individual autonomy as well as

economic opportunity. As industrial countries rely increasingly on information as economic capital, the regulation of personal information takes on new importance. Politically ineffective data privacy policies threaten to spur a privacy revolt, hampering the diffusion of information technologies like e-medical records or responsible data marketing. Affective protection may allay individual concerns while limiting the use of personal information in a range of economic activities. Much like welfare systems, which emerged in the wake of the industrial revolution, the regulation of personal data use will have far reaching implications for the development of industrial economies in the 21st century.