International Review of Law, Computers & Technology

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/cirl20

Global Privacy Concerns and Regulation-- Is the United States a World Apart?

Rita Marie Cain

Published online: 21 Jul 2010.

To cite this article: Rita Marie Cain (2002) Global Privacy Concerns and Regulation-- Is the United States a World Apart?, International Review of Law, Computers & Technology, 16:1, 23-34, DOI: 10.1080/13600860220136084

To link to this article: http://dx.doi.org/10.1080/13600860220136084

International Review of Law Computers & Technology, Volume 16, No. 1, Pages 23–34, 2002

Carfax Publishing
Taylor & Francis Group

Global Privacy Concerns and Regulation—Is the United States a World Apart?

RITA MARIE CAIN

ABSTRACT *The regulatory approach to privacy protection taken by many foreign jurisdictions is markedly different from that of the United States. The European Union (EU) best illustrates the international approach with its comprehensive privacy directive that applies to all EU members. By contrast, the approach regarding data privacy in the United States has been to pass industry-specific laws and often only in response to public outcry over some privacy concern. These fundamental differences have been the source of some conflict in international commercial transacting. Now that the global community is committed to eliminating terrorism, it remains to be seen if these different attitudes toward privacy by the United States and much of the rest of the world will affect global attempts to weed out terrorists. This article discusses the constitutional basis for most US policy approaches to privacy regulation. The article explains how the US constitution is the source for most of the differences between the US and international regulatory approaches to information privacy. Finally, the discussion addresses how new issues regarding privacy in the war on terrorism may be addressed by US Constitutional law.*

Introduction

Prior to 11 September 2001, discussions and research about privacy focused on the privacy of one's personal information in interactive marketing and e-commerce.[1] After the terrorist attacks on the United States, issues about privacy now focus on national security needs to protect against further violence at the hands of individuals among us.

The global community has shown tremendous support for the United States, its citizens and for its resolve to root out terrorist cells throughout the world. Nevertheless, the regulatory approach to privacy protection taken by many foreign jurisdictions is markedly different from that of the United States. The European Union (EU) best illustrates the international approach with its comprehensive privacy directive that applies to all EU

Correspondence: Professor of Business Law, Bloch School of Business and Public Administration, University of Missouri–Kansas City, 5110 Cherry Street, Kansas City, MO 64110, USA. Tel: + 1-816-235-2326, e-mail: cairn@umkc.edu.

ISSN 1360-0869 print/ISSN 1364-6885 online/02/010023-12 © 2002 Taylor & Francis Ltd
DOI: 10.1080/13600860220136084

members. The *European Union Directive on the Protection of Individuals with regard to Processing of Personal Data And of the Free Movement of Such Data* (the Directive) was adopted in 1995 and requires all EU members to have consistent data protection laws.[2] In general, the Directive requires prior, unambiguous consent from individuals for their personal information to be collected or redistributed.[3] By contrast, the approach regarding data privacy in the United States has been to pass industry-specific laws and often only in response to public outcry over some privacy concern. These fundamental differences have been the source of some conflict in international commercial transacting. It remains to be seen if the different attitudes will affect global attempts to weed out terrorists.

This article discusses the constitutional basis for most US policy approaches to privacy regulation. The article explains how the US constitution is the source for most of the differences between the US and international regulatory approaches to information privacy. Finally, the discussion addresses how new issues regarding privacy in the war on terrorism may be addressed by US Constitutional law.

Privacy as an Individual Constitutional Right in the United States

In the United States for the last quarter century the 'right of privacy' has been euphemistic for reproductive freedoms. When the US Supreme Court legalized most abortions in 1973, the Court affirmed that the Constitution includes an implied privacy right.[4] The Court stated that express rights in the Constitution, such as due process, freedom of association and freedom from unreasonable search and seizure emanate from an overarching right of personal privacy.[5] *Roe* v. *Wade* capped a series of mid-20th century privacy cases in the area of intimate personal relations and activities, but acknowledged that privacy had been recognized as a constitutional right since the late 19th century.[6]

The constitutional right of privacy discussed above, however, does not provide consumers any protection against use or abuse of personal data by private sector parties. Data privacy illustrates that the guarantees provided in the Bill of Rights only protect individuals or organizations from government intrusion, not from invasions by private sector parties, such as businesses or non-profit organizations. This limitation, known as the state action doctrine, often is reflected in Bill of Rights language such as: '*Congress* shall make no *laws* abridging freedom of speech …'.[7]

As modern life evolves, the broad statements of fundamental freedoms in the Bill of Rights often need to be more specifically articulated through legislation. Several federal data privacy enactments in the US reflect the general constitutional protection against government intrusion. For example, the Privacy Protection Act of 1980 protects information publishers with search warrant requirements.[8] Thus, this congressional enactment serves to restrict law enforcement from unreasonable search and seizure consistent with the Fourth Amendment of the Constitution and to protect First Amendment free speech and freedom of the press for journalists and authors.[9]

Similarly, the Privacy Act of 1994 restricts disclosure of information held by the US government.[10] The law applies to records that identify a person by name, photo, fingerprint, Social Security number, or voiceprint. This statute requires express consent of the person prior to dissemination of any information. The law also requires examination of the data by the individual subject and an opportunity to correct errors. Thus, this congressional enactment embodies Fifth Amendment due process protections when the government retains and uses personal information in which individuals hold property interests.[11]

Of course, such legislation is always subject to constitutional challenge and judicial interpretation. In particular, claims against the government under these statutes and the governments' asserted defenses based on statutory exceptions, have become the basis for new court opinions on the underlying constitutional rights.[12] In the United States, under the doctrine of judicial review, the courts have the final word when statutory enactments or administrative acts are challenged under the constitution.[13]

Depending on the level and extent of new government intrusions that are imposed in the terrorism war, additional constitutional challenges may arise in response to new enactments. One area of potential regulation that is already receiving attention would permit government agents, such as the Federal Aviation Administration (FAA), to employ racial profiling to distinguish the level of security checks imposed on individuals. Currently, any race-based regulation is analyzed under a 'strict scrutiny' test under the equal protection requirement of the Fourteenth Amendment or the due process protection of the Fifth Amendment.[14] Racial classifications imposed by law are constitutional only if they are narrowly tailored measures that further some compelling governmental interest. Furthermore, racial classifications are highly suspect and presumptively unconstitutional.[15]

Presumably, no level of security risk would justify heightened security measures based exclusively on race under the US Fourteenth Amendment Equal Protection concept. Nevertheless, it is possible that the current security risk is great enough that race could be *one factor* in a series of profiling criteria that might subject an individual to a higher level of government investigation. If the other factors were purely behavioral and not based on national origin, religion or other factors unrelated to criminal activity, then a balancing test that weighs risk against the harm to the individual might justify such an approach.[16]

Another security technique being discussed after the terrorist attacks on the United States is the use of facial scanning and recognition software, to compare faces in crowds at public events or places to existing databases. A similar technology, which scans the iris of the eye, can be used for closer inspection of individuals, such as at ATMs, or for access to secured areas in airports.[17] Fourth Amendment case law in the United States suggests that uses of such technology will likely be permissible for law enforcement purposes. The Supreme Court has upheld aerial observation and photography to be valid investigation techniques, in both business[18] and home settings.[19] The Court's rationale would likely apply to facial scanning and recognition technology used in public places: matters open to public observation are not protected by the Fourth Amendment. Further the Court has held that investigation techniques surrounding free persons who are under no articulable suspicion must be minimally intrusive and justified by law enforcement purposes.[20] Photography and digital scanning by security cameras probably satisfies the requirement of minimal intrusion since the individuals photographed are only captured as they go about their normal course. Use of the techniques at places that may be vulnerable to terrorist attack, such as airports, arenas and government buildings would satisfy the law enforcement requirement.

One worry, however, is that use of facial scanning and recognition technology will be expanded beyond these obviously risky public venues to target certain groups. Thus, any government use of scanning technology to digitally capture all attendees at Muslim mosques could be subject to challenge that the government is racially profiling rather than exercising legitimate law enforcement discretion.

Finally, the Supreme Court recently held that just because a new security or law enforcement technique is technologically feasible does not mean it can be used to circumvent the Fourth Amendment search warrant requirement.[21] In *Kyllo*, the government had

used thermal imaging technology to detect 'hot spots' inside a suspect's home that turned out to be from plant lights used in growing marijuana. Despite the completely unintrusive nature of the technology, the Court held that its use allowed the agents to accomplish, effectively, a warrantless search in violation of the Fourth Amendment. The Court explained that the mere existence of available technology does not justify this kind of search that would otherwise have been unavailable without physical intrusion. Thus, *Kyllo* suggests that the in the United States, the government cannot accomplish through technological means that which would otherwise be unconstitutional if done through old-fashioned police footwork.

The entire foregoing discussion is limited to use of personal information by the government. Despite the widespread discussion of the constitutional right of privacy in modern public dialogue, any protection individuals or organizations are to enjoy from each other must come through legislation passed by the states or the United States. Prior to the terrorist attacks in the United States, the data privacy conversation had focused on the use of personal information by businesses doing marketing and e-commerce. Those issues will continue to require attention since, as is discussed below, the US approach to restricting information collection and use differs from the international community. Further, information collected by businesses for traditional business use, can be subject to subpoena by the government in criminal investigations and prosecutions. If the information had not been collected in the first place it would not be available for law enforcement. Thus, the US and international differences in privacy collection in commerce can affect law enforcement.

A typical US statutory enactment dealing with individual privacy in commerce is the Gramm–Leach–Bliley Act (GLBA) that applies to interstate financial institutions.[22] The statute is an example of how changing times present new privacy concerns. The GLBA is also known as the Financial Services Modernization Act of 1999 because the main purpose of the statute was to modernize financial services offerings by repealing Depression-era laws that prohibited affiliations between banks, insurance companies and securities firms.

After passage of the 1999 law, however, these new, consolidated financial service providers now would have access to personal information among new sister companies. Thus, the GLBA requires these financial services institutions to inform consumers of privacy policies and to notify consumers of their rights to opt out of having personal information shared.[23]

Regulations issued by the Federal Trade Commission (FTC) implementing the GLBA clarify that the term 'non-public information' used in the statute includes information collected by computer 'cookies'.[24] Further, the FTC established that privacy notices must be 'accurate, clear, and conspicuous'[25] and Web site notices must use 'text or visual cues'[26] to attract attention to the notice.[27]

Finally, GLBA allows states to impose more stringent privacy mandates on their local institutions. This additional power to the states illustrates a shared enforcement approach between the United States and the states, particularly in consumer protection laws. Thus, national financial institutions may face as many as 50 different, stricter privacy protection requirements than the federal requirements.

Some evidence from the GLBA privacy notices suggests that U.S. consumers do not have a strong concern about the use of personal data for marketing purposes. Numerous sources have reported scant response from consumers to the opportunity to limit sale or use of their personal data.[28] There is, however, some risk in drawing any universal conclusion about consumer concerns from this data. First, privacy notices under the statute were not required to be in any consistent format or medium. Some institutions sent special privacy mailings,

but others only included the notice as a billing insert, or as a note in a general 'news' piece from the financial institution. Thus, lack of response to the opt-out opportunity may be a product of the poor notice consumers actually received, rather than evidence of consumer attitudes about the collection and use of their data. Meaningful statistical data about the number of informed consumers who declined to opt out of data selling after the first round of mandatory notices on 1 July 2001 is not currently available.

The GLBA is an example of Congress regulating privacy under its power to regulate interstate commerce. Privacy regulation includes a major Supreme Court case on the issue of the federal government's authority under the enumerated powers doctrine, specifically, under the commerce power, which is discussed next.

Congressional Authority to Regulate Data Collection and Use under the Commerce Power

In the United States, the federal government can only regulate those subjects that are specifically enumerated in the Constitution. One such federal enumerated power is the authority to regulate interstate commerce.[29] The commerce power of the U.S. Congress generally has been interpreted quite broadly by the courts in the 20th century. As a matter of fact, today all commercial enterprises, no matter how small or localized, can be regulated by Congress because they 'affect' interstate commerce under current interpretations.[30] Still, under these broad interpretations, it was expected that the regulated activity must be commercial, as opposed to purely charitable, recreational or educational.[31] Arguably, the Supreme Court decision in *Reno* v. *Condon* expresses an even broader view of Congressional authority to regulate data privacy in both commercial and non-commercial settings.[32]

In 1994, Congress passed the Driver's Privacy Protection Act (DPPA).[33] This federal law regulates the states in their disclosure of personal information contained in motor vehicle department (DMV) records. Prior to the DPPA, the information that drivers must provide to receive a driver's license and to register their vehicles was widely sold to industry for surveys, marketing and other purposes. The Supreme Court noted that Wisconsin received almost US $8 million annually from the sale of this information.[34]

The DPPA restricts the states' right to sell this information without the prior approval of the driver. Such a system of affirmative approval is described as an 'opt-in' system. The states must ask the subjects if they want their data included in the information disclosed and the subjects must affirmatively agree. Presumably, in this era of increasing concern over privacy, not many citizens would agree to this sale of their information. Thus, an opt-in system puts lesser burden on the subjects of the information to accomplish their likely privacy wishes. The information cannot be sold unless the consumer proactively allows it.[35]

South Carolina challenged the law because disclosure provisions in its state laws directly contravened the federal mandate. South Carolina's DMV records were available to anyone who filled out a request form and confirmed that the records would not be used for telephone solicitations. South Carolina allowed drivers to restrict use of their information, in a system commonly described as 'opt-out'. The subject had to proactively request their information be excluded from disclosure.

Condon was widely watched among interactive marketers because motor vehicle information was commonly purchased for targeted solicitations. Industry observers were concerned about the impact the federal limitations would have on the availability of this

oft-used information. States and states' rights advocates were interested in the case because it represented issues of federalism v. states' rights.

In *Condon*, the Supreme Court noted that the relevant data were used by both public and private parties engaged in interstate commerce. As such, the Court declared the information is 'an article of commerce, its sale or release into the interstate stream of business is sufficient to support congressional regulation'.[36] The Court stated it was not necessary to determine whether use of the information has a substantial impact on interstate commerce, the test frequently applied to test the constitutionality of federal legislation. Accordingly, the case stands in marked contrast to most 20th century cases regarding the scope of the commerce power, which applied the 'affects' test to uphold the regulation under the commerce clause.

Upon a reading of *Condon*, one must ask, what, if any, collections and uses of data would *not* be subject to the federal power as articulated in *Condon?* The Court's description of the DMV data and its use by commercial and non-commercial parties 'in the stream of interstate commerce …' would seem to apply to any data that is systematically collected and reused by any organization. The commercial nature of the users no longer is important.

Finally, the *Condon* Court's broad statement of authority also appears *not* limited to the *sale* of information even though that was the activity at issue in the case. For example, the Court stated that this particular data was 'released' for matters related to 'interstate motoring'. The Court seems to be saying that dissemination of data in relation to any activity that can be characterized as 'interstate' leads to the conclusion that the data is 'an article of commerce …'. Sale of the information is not required.

Condon firmly establishes the federal right to broadly regulate data collection and dissemination under the Commerce Power. Yet, that proper exercise of authority under the commerce power does not immunize legislation from other challenges under the Bill of Rights. One such constitutional challenge was successfully asserted in *U.S. West, Inc.* v. *FCC*.[37] This case analyzed whether privacy regulations enacted by the Federal Communications Commission (FCC) under the Telecommunications Act of 1996 violated the First Amendment commercial speech rights of the telephone companies.

In the United States, the right to advertise goods and services is protected free speech under the constitution.[38] Advertising, also called 'commercial speech' in the first amendment analysis, receives slightly less protection than political or social speech. Nevertheless, any regulation limiting a commercial party's promotional message to its customers will undergo significant judicial scrutiny.[39]

In *U.S. West*, the FCC regulations required telephone companies to gain customers' permission prior to using customer proprietary network information (CPNI) for marketing purposes. In other words, just like the DPPA in *Condon*, the regulations created an 'opt-in' scheme, contrary to the typical opt-out approach used in self-regulation by most industries, before they could target direct marketing messages to their customers based in the CPNI.

U.S. West illustrates the analysis courts apply when a government regulation is challenged under the constitution. First, the government must assert a substantial state interest that it seeks to protect with the challenged regulation. Many may be surprised to discover that the court disputed the government's assertion that individual privacy was a substantial interest *per se*.[40] In fact, the court engaged in an analysis seldom heard: the downside of privacy protection. The court stated: 'privacy is not an absolute good'.[41] The court was eerily prescient when it explained that privacy imposes costs on society including the ease of perpetrating crimes based on false information and increased difficulty prosecuting such

crimes.[42] Certainly, in a world at war with terrorists, many citizens may believe that future law enforcement needs are superior individuals' concern about secrecy of their personal information.

In the more mundane world of commerce, there also is a price for privacy protection, according to the *U.S. West* court. When privacy rights interfere with businesses' collection and use of information, it reduces efficiency in markets. In such cases, privacy could lead to lower productivity and increased prices.

For the purpose of this appeal, however, the *U.S. West* court reluctantly accepted that the privacy interest was a substantial state interest that warranted protection through government regulation.[43] Regardless, the court concluded that opt-in scheme in the FCC regulations did not fit the second prong of the constitutional analysis, the requirement that the regulations be properly tailored to address the alleged risk.

U.S. West is enlightening regarding the level of concern the US public actually has about the privacy of their personal data. The FCC presented U.S. West's own study that 33% of customers refused to 'opt in' when called and asked for permission. Another 39% either hung up or asked not to be called again. From this information, the FCC argued that an opt-in system properly addresses customer privacy concerns since a majority of customers had failed to give the necessary permission. In the same study, 28% had granted the necessary approval.

On the other hand, separate data showed that when *customers* initiated the contact with the telephone company themselves, a startling 72% approved use of their CPNI. According to the court, all these results suggested consumer ambivalence or disinterest in the privacy concern.[44] The court opined that the customers who were called and responded negatively might be averse to telemarketing, not to the use of their CPNI.[45] Accordingly, this statistical evidence did not support the stringent opt-in system when the more conservative approach, an opt-out system, could suffice to meet consumer concerns. As such, the court ruled that the FCC regulations were based on speculation and did not reflect the necessary weighing of costs and benefits by the government that the First Amendment free speech right requires.[46] Thus, at least one court would not assume anything about how concerned individuals actually are about the privacy of their personal data.[47]

The US constitutional law of privacy regulation could be summarized as follows: (1) Privacy is an individual constitutional right that warrants some restrictions on government intrusion; (2) *Condon* laid the foundation for comprehensive federal data regulation across all sectors of US life; (3) broad regulations limiting customer contact, when based on mere assertions of consumer privacy concerns, will not pass First Amendment scrutiny. The latter conclusion supports commentators who opine that comprehensive legislation regarding data collection and use is not likely in the offing for the United States, which puts US law in direct conflict with the EU approach.[48]

The International Approach to Privacy Regulation: Learning through Comparison and Contrast

Since the 1970s, countries have established 'fair information principles' or FIPS to govern data protection. Some of the basic principles include (1) giving consumers notice about or control over the collection and use of their information; (2) giving consumers access to information and a right to correct discrepancies; and (3) ensuring the security of data when held and used by governments or third parties.[49] These principles are embodied in FTC Guidelines, in US sector-specific laws, in Guidelines established by the Organisation for

Economic Cooperation and Development (OECD)[50] as well as in the EU Directive. They usually provide the framework of any self-regulatory approach. The principles do not dictate that governments adopt comprehensive regimes to ensure national enforcement. Nevertheless, that has been the approach of the EU.

The EU Directive mandates member states to adopt laws requiring, among other things, that personal data be processed fairly and lawfully, that data be collected only for express, legitimate purposes and not be further processed in ways inconsistent with those purposes, nor kept for longer than those purposes require, and that data be accurate and current (and if not, are deleted or corrected).[51]

The additional mandate of the EU Directive that radically departs from US law is that member states only permit processing of personal data if 'the data subject has unambiguously given his consent …'.[52] Although the Directive provides exceptions to the consent requirement, including one in which the data processing is necessary for the performance of a contract with the data subject, the general approach is an 'opt-in' system, akin to that rejected by the court in *U.S. West*.

Further, the Directive goes on to completely prohibit processing of data that that reveals 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'.[53] Time remains to tell if the EU will consider easing this restriction to aid in the search for terrorist groups. In particular, law enforcement officials might want to see financial institutions collect such information for the purpose of linking individuals to terrorist activities in support of the global effort to choke off sources of financial support for terrorist activities.

The EU Directive illustrates how the global marketplace can create a global regulatory environment. The Directive only permits EU members to transfer data to a party in another country if that country has in place an 'adequate level of protection' for personal data. In other words, the European Community is imposing its standards and values regarding privacy on the rest of the world, by limiting European businesses from transacting with foreign firms, if those firms' domestic laws do not align with the EU mandates of privacy protection. Among other things a country's 'adequate level of protection' is measured by 'rules of law, both general and sectoral' and 'professional rules and security measures which are complied with in that country'. In other words, for trading partners to do business with European firms, privacy protection must be enforced in the trading partner's home country.

In response to the requirements of the EU directive for non-EU trading partners, Canada passed national privacy legislation that took effect 1 January 2001.

By contrast, the US has no general privacy laws, and sectoral laws currently are limited to telecommunications, health care and financial services (including credit reporting). The US has no centralized agency for privacy enforcement. Thus, industry self-regulation for most US businesses must suffice for 'professional rules and security measures'. European and US businesses have been concerned that EU officials would be dissatisfied with that level of protection and begin to block data transfers to the US.

Accordingly, the Commerce Department negotiated safe harbor provisions with the EU for US firms to satisfy in order to avoid the EU blocking data transfers to the US. The safe harbor provisions are primarily a uniform system of self-regulation and enforcement, although they include a fallback complaint mechanism to the Federal Trade Commission (FTC) under its authority to pursue deceptive trade practices. Terms of the safe harbor require firms to contractually agree, among other things, to notice and opting out mechanisms. Opt-in opportunities must be provided for the use of the sensitive data

discussed above. The Department of Commerce will maintain a list of all firms that certify they meet the safe harbor provision.

There is considerable written debate in business, legal and international publications about the value of the competing US and EU approaches to data privacy protection. For example, Consumers International studied 750 internet sites to determine how much information is collected from internet users and to see what steps are taken to protect the privacy of this information. One of the objectives of the study was to establish whether there was significant difference between EU and US-based sites.[54] The study concluded that, despite comprehensive EU legislation, 'U.S.-based sites tended to set the standard for decent privacy policies' and gave better information or a higher degree of choice to users.[55]

Despite this finding, the study still faults the US sectoral approach to privacy legislation because it lacks any common oversight agency. Further, self-regulation, which is the only constraint for most US e-retailers, is faulted for lacking minimum standards, proper notice to consumers and the ability of the site operator to abandon or change the policies at will.[56] The study also criticizes the U.S. Commerce Department safe harbor provisions because the safe harbor provisions are based on self-regulation and lack adequate enforcement.[57]

Another author discussed the differing approaches of the US and EU and concluded neither vehicle provided adequate consumer protection: 'The net-effect is that e-commerce has become a tangled web of policy, regulations and unforeseeability—an area ripe for e-consumer harm'.[58] Aguilar concludes that the continued debate about the differing US and EU approaches is part of the problem: 'These competing visions will result in no e-consumer protection and an inability for e-businesses to stave off litigation.'[59] He proposes 'Government Enforced Self-Regulation.' This hybrid approach can take on various forms, such as industry participation in legislative drafting where industry standards are elevated to the force of law. In the US, state and local building codes often are developed this way. Alternatively, industry or other self-regulatory enforcement processes can be government sanctioned and operate with the force of law. Examples of such processes already in effect in the US include arbitration of disputes by the National Association of Securities Dealers, which is authorized by the federal securities laws, and the Better Business Bureau new car 'lemon law' arbitration process, which satisfies FTC regulations.

In comparing and contrasting the US v. EU approach, readers should consider the possibility of an approach that is even more *laissez faire* than the current US safe harbor provisions.[60] Such an alternative would make the availability and use of information purely a matter of individual enforcement under contract law. As the author explains it:

> Current solutions to online privacy fail to give consumers control over how their information is used or compensation for the data they share. ... an online licensing system based on the Uniform Computer Information Transaction Act (UCITA) can achieve these objectives. Individuals will contract with businesses for the right to use their personal information. The licensing terms they negotiate will set limits on how their data is used, how long it is used and what type of benefit it is exchanged for.[61]

Admittedly, such a system of purely private enforcement gives consumers control over and the potential to profit from the use of their data. Nevertheless, it could prove unrealistic for many consumers.[62] While most regulatory schemes attempt to lessen the enforcement burdens on consumers, a purely private scheme ignores that common goal and increases that burden, which could prove unsatisfactory when dealing with foreign parties under the EU scheme.

Conclusion

Until 11 September 2001, the discussion about privacy regulation centered almost exclusively about uses of personal information in e-commerce. Now the conversation is centered around law enforcement and government access to information.

In the United States, when the debate is limited to access and use of data by private parties, the conclusions are fairly clear cut: (1) Congress has the authority to regulate most, if not all, data collection and use; (2) businesses who seek to use customer data to craft a targeted message have a right to do so under the First Amendment commercial speech doctrine; (3) any restriction on access to data will be in an 'opt-out' system, whereby consumers must take the initiative to block collection or use of personal information; and (4) the vast majority of consumers are not motivated to exercise those opt-out rights.

When the debate moves to collection and use of data for law enforcement purposes, the conclusions are muddied. Current case interpretations of individual constitutional rights suggest that collecting religious and racial profiling data to respond to terrorism would be deemed unconstitutional. However, no one knows how much weight a court, including the U.S. Supreme Court will place on the unusual risk posed by terrorists among us, who can carry out their violence with instruments from our everyday lives. By contrast, non-intrusive uses of scanning technology will be permissible.

Equally intriguing is the question of international attitudes toward privacy protection and whether they will modify in an era of increased security concerns. As the court in *U.S. West* pointed out, privacy protection is not an absolute right and can fly directly in the face of the need for criminal investigations and security. Whether the EU will consider easing its restrictions on data collection and dissemination to serve the increased security need remains to be seen.

References

1 PM Schwartz 'Commentary: internet privacy and the state' *Connecticut Law Review* Vol 32, p 815, Spring 2000. See also, FH Cate 'Commentary: principles of internet privacy' *Connecticut Law Review* Vol 32, p 877, 2000.
2 EUR-Lex 'Community Legislation in Force' Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (last modified 3 November 1999) http://europa.eu.int/eur-lex/en/lif/dat/1995/en 395L0046.html [hereinafter Directive]. See *supra* notes 50–57 and accompanying text.
3 *Ibid.* at art. 7(a).
4 *Roe* v. *Wade*, 410 U.S. 113 (1973).
5 *Ibid.* at 129.
6 *Ibid.* at 152.
7 U.S. Constitution, Amendment I.
8 Privacy Protection Act of 1980, 42 U.S.C. sect. 2000 (2000).
9 In fact, the Privacy Protection Act of 1980 created additional statutory protections for news organizations than the Supreme Court previously had articulated under the First Amendment. The legislation was perceived to be a direct response to the Court's decision in *Zurcher* v. *Stanford Daily*, 436 U.S. 547 (1978) in which the court upheld a warrantless search of the newspaper offices.
10 Privacy Act of 1994, 5 U.S.C. sect. 552(a) (2000).
11 See e.g. *Sherman* v. *United States Dept of the Army*, 244 F.3d 357 (5th Cir. 2001), which emphasized an individual's significant privacy interest in their social security number.
12 See e.g. *National City Trading Corp.* v. *U.S.*, 635 F.2d 1020 (2d Cir. 1980) (upholding the terms

of a search warrant under the Fourth Amendment when the defendant challenged it under the 1980 Act). See also, *Adams* v. *City of Battle Creek*, 250 F.3d 980 (6th Cir. 2001) (striking down a wiretap of a police officers pager, despite a 'law enforcement' exception in the Electronic Communications Privacy Act).

13 *Marbury* v. *Madison*, 5 U.S. (1 Cranch) 137 (1803).

14 Adarand Constructors, Inc. v. Pena, 515 U.S. 200 (1995).

15 *Ibid.*

16 In affirmative action (also known as 'reverse discrimination') cases, race has been permitted as one of numerous factors in awarding college admissions or other government contracts. However, the racially-based programs could only be used to remedy actual past discrimination by the government. In other words, when race is used as a factor for discriminating among individuals for it, the justification has to be real, not speculative. *Shaw* v. *Reno*, 509 U.S. 630 (1993).

17 See, 'Iris scans replace PINs, passwords' *Corrections Professional* Vol 7, 21 September 2001 (explaining that iris scanning is in use in a Pennsylvania prison, at ATMs in Texas, and at the Charlotte, North Carolina airport). See also, 'Biometric facial recognition to target corrections *Corrections Professional* Vol 6, 20 October 2000.

18 *Dow Chemical Co.* v. *United States*, 476 U.S. 227, 237 (1986).

19 *Florida* v. *Riley*, 488 U.S. 445, 449 (1989); *California* v. *Ciraolo*, 476 U.S. 207 (1986).

20 *Michigan State Police* v. *Sitz*, 496 U.S. 444 (1990); *Hayes* v. *Florida*, 470 U.S. 811 (1985).

21 *Kyllo* v. *United States*, 121 S.Ct. 2038 (2001).

22 Public Law Number 106–102, 113 Stat. 1337 (12 November 1999).

23 *Ibid.* at Title V.

24 16 C.F.R. sect. 313.3(b)(1)(F) (2001).

25 16 C.F.R. sect. 313.3(b)(1) (2001).

26 16 C.F.R. sect. 313.(b)(1)(iii) (2001).

27 See J Hiller and R Cohen *Internet Law and Policy* Prentice Hall, 2002, p 82.

28 WA Lee 'Opt-Out Notices Give No One a Thrill' *The American Banker* 10 July 2001.

29 U.S. Constitution, Article 1, Section 8.

30 *Wickard* v. *Filburn*, 317 U.S. 111 (1942); *Heart of Atlanta Motel* v. *U.S.*, 379 U.S. 241 (1964).

31 One of the few modern commerce power cases to strike down the federal regulation is found in *U.S.* v. *Lopez*, 514 U.S. 549 (1995). The statute at issue in *Lopez* was an attempt to address gun violence in and around schools. This comprehensive gun possession law prohibited possession of a gun within 1000 feet of a school. According to the law, all gun possession close to a school threatened the United States' ability to educate its youth and, thus, its future ability to compete in world markets. Accordingly, such gun possession affects interstate commerce and could be regulated by Congress. Not so, according to the U.S. Supreme Court, which found this to be a comprehensive regulation of public safety, normally a matter for the U.S. states not for the federal government.

32 *Condon* v. *U.S.*, 528 U.S. 141 (2000).

33 Driver's Privacy Protection Act, 18 U.S.C. sect. 2721–25 (2000).

34 528 U.S. at 144 (citing *Travis* v. *Reno*, 163 F.3d 1000, 1002 (7th Cir. 1998)).

35 The statute makes exceptions for all state use of the information to carry out governmental functions. The statute also allows for limited disclosure to industry for purposes such as product recalls, performance monitoring and research. The statute, however, restricts the reuse or resale of information received under these exceptions. The statute imposes criminal penalties for intentional violators and creates a civil action for drivers whose information is wrongfully disclosed. 18 U. S. C. sect. 2721 (b) (2001).

36 528 U.S. at 149.

37 182 F. 3d 1224 (10th Cir. 1999).

38 Virginia Board of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976).

39 See e.g. *Cincinnati* v. *Discovery Network*, 507 U.S. 410 (1993).

40 182 F. 3d at 1234–36.

41 *Ibid*. at 1235.
42 The court also explained that privacy protection can threaten public safety by reducing access to information about an individual's history of child abuse, sexual offenses, or communicable diseases. *Ibid*.
43 *Ibid*. at 1239.
44 *Ibid*.
45 *Ibid*.
46 *Ibid*.
47 The court's approach would seem to be supported by new information about U.S. taxpayers' actions regarding access to their tax preparation information. For the first time in 2000, taxpayers were given the opportunity to check a box to allow the Internal Revenue Service (IRS) direct contact with the individual who prepared the taxpayer's federal income tax return. Although the statutory authority for this permission actually limited the IRS to certain subjects for inquiry from the preparer, the actual form by which permission was granted from the taxpayer explained no such limitation. Further, the IRS could contact the tax preparer without the taxpayer being notified of the interaction. In other words, for all he/she knew, the taxpayer could be authorizing federal revenue officials *carte blanche* to secretly investigate the taxpayer through access to this knowledgeable and formerly confidential, source. Readers might assume that few taxpayers would give the government this expansive investigative right. Quite the contrary! The IRS reported that over 30 *million* U.S. taxpayers authorized the IRS to interview their tax preparer. Most do not want to be bothered to even know that their tax return is under this kind of scrutiny. Thus, in this most sensitive area of financial disclosure many U.S. citizens are unconcerned about loss of privacy and confidentiality. *Tax Notes Today* pp 185–184, 24 September 2001.
48 M Johnston 'Legislators use caution in tackling privacy' *Infoworld* Vol 22, No 12, p 26, 20 March 2000.
49 J Berman and D Mulligan 'The internet and the law: privacy in the digital age: work in progress' *Villanova Law Review* Vol 23, p 549, 1999.
50 Organisation for Economic Development and Cooperation, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980) available at http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.
51 See *supra* note 3 at art. 6.
52 *Ibid*. at art. 7(a).
53 *Ibid*. at art. 8(1).
54 K Scribbins 'Privacy@net, an international comparative study of consumer privacy on the internet', at 5 (January 2001) (found at http://www.consumersinternational.org/campaigns/index.html#electronic).
55 *Ibid*. at 6.
56 *Ibid*. at 31–32.
57 *Ibid*. at 15.
58 JR Aguilar 'Over the rainbow European and American consumer protection policy and remedy conflicts on the internet and a possible solution' *International Journal of Communication Law & Policy* Vol 4, p 1, Winter 1999/2000.
59 *Ibid*. at 54.
60 K Basho 'Comment: The licensing of our personal information: is it a solution to internet privacy?' *California Law Review* Vol 88, p 1507, 2000.
61 *Ibid*. at 1507.
62 PP Swire and RE Litan *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* Brookings Institution Press, 1998, p 8.