Privacy Regulation

Spring 2004

Table of Contents

Consumer Protection Committee
Computer and Internet Committee
Section of Antitrust Law
American Bar Association

Privacy Regulation

Spring 2004

Editor-in-Chief

D. Reed Freeman, Jr.
Collier Shannon Scott PLLC
Washington, DC
rfreeman@colliershannon.com

Editors

Peder Magee
Federal Trade Commission
Washington, DC
pmagee@ftc.gov

Ponneh Aliabadi
Collier Shannon Scott PLLC
Washington, DC
paliabadi@colliershannon.com

Alysa N. Zeltzer
Collier Shannon Scott PLLC
Washington, DC
azeltzer@colliershannon.com

Privacy Regulation is published two times a year by the American Bar Association Section of Antitrust Law Consumer Protection and Computer and Internet Committees. The views expressed in the Newsletter are the authors' only and not necessarily those of the American Bar Association, the Section of Antitrust Law, or the Consumer Protection and Computer and Internet Committees (or their subcommittees).

If you wish to comment on the contents of the Newsletter, please write to the American Bar Association, Section of Antitrust Law, 750 North Lake Shore Drive, Chicago, IL 60611.

From the Editor

The Computer and Internet Committee and the Consumer Protection Committee of the American Bar Association's Antitrust Section are pleased to announce the publication of the Spring 2004 edition of Privacy Regulation. This issue includes four articles, three of which focus on international privacy issues and one of which is focused on information security.

The first article, by Michael Fekete and Patricia Wilson of the Toronto and Ottawa offices, respectively, of Oslar, Hoskin, & Harcourt, LLP, focuses on Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and similar provincial legislation.

Marcus Turtle of Field Fisher Waterhouse in London follows with a discussion of the regulation of email marketing under the UK's Privacy and Electronic Communications regulations, which came into effect on December 11, 2003.

The third article, by Jon G. Filipek of the Brussels offices of Weil, Gotshal & Manges, LLP, addresses on the European Commission's "First Report on the Implementation of the Data Protection Directive (95/46/EC)." The article focuses on the divergent approaches taken by various EU Member States on issues including when third-country transfers are permitted under Member State laws implementing Articles 25 and 26 of the Directive, and describes the European Commission's Work Programme for a Better Implementation of the Data Protection Directive.

This issue concludes with an article by Leslie F. Spasser of Wilcox & Savage in Norfolk, Virginia, on the development of legal standards for information security in broadband applications. The article gives a background on federal and state security standards and enforcement actions and offers ways to broadband providers to minimize their risk in this evolving area of the law.

I would like to thank the members of our Editorial Board - Peder Magee, Attorney Advisor to FTC Commissioner Mozelle Thompson, and Alysa Zeltzer and Ponneh Aliabadi, both of Collier Shan-

non Scott, PLLC – for their work to make sure that the articles we publish are accurate, complete, and, most importantly, focused on assisting privacy practitioners in their day-to-day work.

We hope that you find this issue useful in your practice. If you have any questions, comments, or suggestions for improvement, please let me know.

D. Reed Freeman, Jr.
Collier Shannon Scott PLLC
Washington, DC
rfreeman@colliershannon.com

Privacy
Regulation

Spring 2004

PIPEDA – A Clearly Canadian Approach to Privacy Protection

Michael Fekete[1]
Osler, Hoskin & Harcourt LLP
mfekete@osler.com

Patricia Wilson[2]
Osler, Hoskin & Harcourt LLP
pwilson@osler.com

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal government of Canada's contribution to the international proliferation of private sector privacy legislation. Although it draws heavily from internationally recognized privacy principals, PIPEDA is clearly and uniquely Canadian. Identifying these "Canadianisms" is critical to understanding how PIPEDA is changing the privacy landscape in Canada.

The Influence of Europe

Canada has a long-standing tradition of looking to the other side of the Atlantic (principally to the UK) to borrow models for legislation, rather than to its neighbour south of the border. PIPEDA represents a continuation of this tradition. Instead of following the U.S. approach, where privacy concerns have largely been dealt with on a more selective basis on the federal level (*e.g.*, through misleading advertising and other sectoral-based laws such as HIPAA and Gramm-Leach-Bliley), Canadian legislators have drawn more closely from the European privacy law model, with its inclusion of "fair information management principles" developed in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

Under PIPEDA, there are detailed rules which govern the management of personal information in the course of commercial activities. Organizations must advise individuals of the purposes and obtain their consent for the collection, use, or disclosure of their personal information. The purposes themselves must be reasonable and appropriate. Personal information can only be used

for the purposes for which it was collected and should not be retained by the organization longer than needed for those purposes. If an organization is going to use the information for another purpose, consent must be obtained again.

The individual has a right to access personal information held by an organization and to challenge its accuracy. Personal information in the custody of organizations must be protected by specific safeguards, including physical and technology-based security measures commensurate with the sensitivity of the information. Individuals have a right to complain and seek redress for breaches of the fair information privacy principles.

PIPEDA makes Canadian organizations accountable for the use and disclosure of personal data they've collected through service providers, data processors, or outsourcing arrangements. For example, under PIPEDA, Canadian organizations are responsible for third-party contractors, including those located outside Canada, and must make sure that adequate contractual protections to ensure compliance with PIPEDA are in place.

However, PIPEDA doesn't go quite as far in attempting to control global flows of personal information as does the EU's "safe harbour" rule. This directive requires organizations to ensure that any jurisdiction to which they are sending personal data about employees, customers, etc., has enacted legislation that offers "adequate" privacy protection. Nor does Canadian law require businesses that collect or disseminate data to register with an agency as does the EU. Despite these differences, the EU approved PIPEDA as satisfying the requirements of its trans-border data flow directive in January 2002, subject to further review of provincial privacy legislation when enacted.

Consensus – Based Code of Privacy Practices

PIPEDA is highly unusual legislation in that it incorporates the "Model Code for the Protection of Personal Information" developed by the Canadian Standards Association. As its name suggests, the model code was not drafted as proposed legislation. It sets out a flexible approach to privacy protection and, in many instances, provides best practices for protecting personal information, rather than mandatory rules.

The decision to incorporate the Code into PIPEDA (with only a handful of provisions being overridden) reflected a desire to build consensus on the legislation among privacy advocates and private sector organizations. A wide spectrum of interests were directly involved in or consulted during the preparation of the Code. As a

result, it was positioned by the federal government as a "ready-made" solution.

Conciliation-Based Dispute Resolution

Although it has been in force since January 1, 2004, there have been no damages awards or fines issued under PIPEDA. In contrast, during the same timeframe, the enforcement of misleading advertising laws in the U.S. have resulted in a significant number of high-profile, high-dollar value prosecutions and consent-decrees in respect of unlawful privacy practices.

Oversight of PIPEDA rests with the Privacy Commissioner of Canada, whose office investigates complaints and negotiates solutions with the parties involved. The Commissioner does not have the authority to make binding orders or award damages, but issues recommendations to organizations found to be non-compliant. An individual complainant and, in limited circumstances, the Commissioner have standing to apply to the Federal Court of Canada for binding orders requiring compliance and, in the case of individuals, damages. Only a handful of applications have been made.

The role adopted by the Commissioner has been similar to that of an ombudsperson, combining public education with efforts to find "fixes" for privacy breaches which strike a balance between the rights of individuals to have their personal information protected and the legitimate needs of organizations to collect, use, and disclose it. This is not say that the Commissioner has been unwilling to take forceful positions on significant issues; many of the more than 220 findings issued to date will have a material impact on "industry standard" business practices (*e.g.*, opt-out consent, sharing of customer information by affiliates, and the taping of customer telephone calls). However, in keeping with the goal of finding solutions in a non-adversarial manner, as a general rule, the Commissioner has not disclosed the identity of the target of complaints. Jennifer Stoddart, the recently-appointed Commissioner, has undertaken to review this practice of former Commissioner George Radwanski, but she has also gone on the record with a commitment to work closely with organizations as they struggle with the challenges of complying with PIPEDA.

Federal-Provincial Turf

Canada's federal structure has resulted in no shortage of turf wars between the federal and provincial levels of government. While the Constitution gives the federal government jurisdiction over limited areas which impact on business, including criminal law and national

and international trade and commerce, most local business activities fall within the domain of the provinces.

This allocation of jurisdiction is reflected in an exclusion within PIPEDA and its phased introduction. With respect to the exclusion, PIPEDA does not apply to organizations in relation to their employees unless they are "federal works or undertakings" (such as banks, telecommunications carriers, broadcasters, and interprovincial transportation companies). This takes into account that laws in respect of employees of provincially regulated organizations clearly fall within the jurisdiction of the provinces.

Regarding the phased introduction of PIPEDA, federal works and undertakings have been subject to PIPEDA since January 1, 2001, whereas the privacy practices of their provincially regulated counterparts have been within the reach of PIPEDA only since January 1, 2004. This was done to give the provinces an opportunity to enact their own version of privacy legislation, failing which PIPEDA would come into effect. If the federal government declares that "substantially similar" privacy legislation is in place in a province, PIPEDA does not apply to the protection of personal information within the province.

As indicated in the summary of provincial privacy laws below, only three provinces (Québec, British Columbia, and Alberta) have enacted private sector privacy legislation and, at the time of writing, only the legislation in the province of Quebec had been declared by the federal government to be substantially similar to PIPEDA. Further, the phased introduction of PIPEDA has not been successful at avoiding a turf war on jurisdictional grounds. The Québec government recently launched a constitutional challenge to PIPEDA; specifically, the exemption process whereby provincial laws are subjected to federal review for substantial similarity to the federal standard has been targeted. It is not yet known when the challenge will be heard.

Even if the "substantially similar" issues are settled, the complexities caused by dual levels of privacy laws will not be eliminated. PIPEDA will continue to apply to the federally regulated businesses, even in provinces with substantially similar legislation, and to the interprovincial collection or disclosure of personal information into or from any province. Further, Québec's privacy law makes organizations responsible for compliance when they use or disclose personal information outside of the province. Barring any clarification by the federal and provincial privacy commissioners, this apparent overlap is likely to create a degree of confusion over which body - federal or provincial - has jurisdiction where data flows outside a province are concerned.

Cross-Country Summary of Provincial Laws

British Columbia: British Columbia has enacted private sector privacy legislation, the Personal Information Protection Act, which came into force on January 1, 2004. This legislation applies to the private sector in British Columbia (both profit and non-profit organizations) and covers personal information of individuals whose information the organization holds and employees of the organization. It does not apply in situations where PIPEDA applies. The federal government has yet to decide whether the Personal In formation Protection Act is "substantially similar" to PIPEDA, so as to preclude the application of PIPEDA within the province in favour of the provincial legislation. Private sector organizations in British Columbia are therefore subject to both PIPEDA and the British Columbia legislation.

Alberta: Alberta enacted the *Personal In formation Protection Act* which came into force on January 1, 2004. This legislation applies to the private sector in Alberta in respect of all commercial activity, although it has only limited application to non-profit organizations, and will cover personal information of both individuals whose information the organization holds and employees of the organization. The federal government has yet to decide whether this legislation is "substantially similar" to PIPEDA, so as to preclude the application of PIPEDA within the province in favour of the provincial legislation. Alberta has also enacted a health information protection law covering both the private and public sectors that is now in force. Private sector organizations in Alberta are therefore subject to both PIPEDA and the Alberta legislation.

Saskatchewan: The province has enacted a health information protection law covering the public and private sectors that was declared in force (except for certain provisions) as of September 1, 2003. Saskatchewan has made no move to introduce general privacy legislation covering the private sector. Again, private sector organizations are, as of January 1, 2004, subject to PIPEDA, at least with respect to non-health information, in the province on January 1, 2004.

Manitoba: The province has enacted a health information protection law covering the public and private sector that is now in force, but has made no move to introduce legislation covering the private sector. Therefore, private sector organizations, are, as of January 1, 2004, subject to PIPEDA, at least with respect to non-health information, in the province on January 1, 2004.

Ontario: The province introduced a bill addressing personal health information on December 17, 2003. Although the Ontario government released a draft privacy bill for consultation in 2002, it

failed to introduce private sector privacy legislation due to ongoing concerns about the draft legislation. It is unclear if or when the new provincial government will pass "made in Ontario'' privacy legislation. Private sector organizations in Ontario are, as of January 1, 2004, subject to PIPEDA, in respect of health and non-health information about individuals.

Québec: Québec has had private sector privacy legislation in place since 1994. Its Act Respecting the Protection of Privacy in the Private Sector is also based on the "fair information principles" set out in the OECD Guidelines and is similar in its requirements to PIPEDA. The legislation applies to all private sector organizations with respect to the personal information of all members of the public and of employees. It also applies to private sector collection, use, or disclosure of personal health information.

Atlantic Provinces: None of Newfoundland, Nova Scotia, Prince Edward Island, or New Brunswick has announced plans to introduce private sector provincial privacy legislation as of January 2004. Private sector organizations in these provinces are, as of January 1, 2004, subject to PIPEDA.

Yukon, Nunavut, and Northwest Territories: None of Canada's three territories has introduced or enacted privacy legislation applicable to the private sector. As federal territories, PIPEDA applies to businesses in the territories, with respect to both their customers and employees.

P

(Endnotes)

1 Michael Fekete is a partner in the Business Law Department in Osler, Hoskin & Harcourt LLP's Toronto office, practising in the Technology Business Group. Michael's practice focuses on information technology, software development and licensing, e-commerce and privacy.

2 Patricia Wilson is a partner in the Litigation Group in Osler, Hoskin & Harcourt LLP's Ottawa office, practising in the area of public and administrative law. Patricia has developed extensive litigation and advisory expertise in access to information and privacy law.

Privacy
Regulation
Spring 2004

New Rules for Marketing by Email and Text Message

Marcus Turtle[1]
Field Fisher Waterhouse
London, England
Marcus.Turtle@ffw.com

New rules came into force on December 11, 2003 that add a further layer of regulation to the way companies market using electronic communications. At the moment, regulations principally address marketing through email and text message, but they will also cover picture and video messaging when these come fully online. The use of cookies and location data will also be regulated.

The Data Protection Act 1998 already governs the way we use information which identifies people, but the new rules go further. One fundamental change, intended to assuage the Orwellian fears of consumers and privacy advocates, is that for some categories of information, even data that is non-personally identifying will be caught. This presents a significant challenge for companies who market to consumers. The rules for cookies will affect even those whose business models are exclusively b2b.

The Privacy and Electronic Communications Regulations 2003 implement in the UK the Directive of the same name. Although passed in September, the new rules did not actually come into effect until December 11, 2003, so there have been only a few weeks of experience with the new regulations.

Unsolicited Direct Marketing

The Regulations apply to the sending of direct marketing messages by electronic means. The phrase "electronic means" is intentionally broad in meaning, so that the Regulations will cover new developments in electronic communications as and when they come online. "Direct marketing" covers a wide range of activities, applying not just to the offer for sale of goods and services, but also to the

promotion of an organization's aims and ideals. It probably includes, for example, a charity or political party making an appeal for funds or support.

"Unsolicited" direct marketing should also be distinguished from solicited marketing. The latter is marketing that you have actively invited; the former is not – it is marketing that you have positively indicated you do not mind receiving. The Information Commissioner, the UK's privacy watchdog, provides the following analogy: unsolicited versus solicited marketing is akin to the difference between asking someone to buy you a drink and that person asking you if they *may* buy you a drink, to which you answer "yes." The outcome may be the same, but the process leading up to it is not. So, if you email a travel agency and ask them to look into the cost of flights to Prague at New Year, you are soliciting a reply from the travel agency with a range of quotes for that trip. The travel agency could send you further marketing emails about other flights to other destinations at a later date which *they* think might interest you. These would be unsolicited and would now be covered by the Regulations.

In essence, the Regulations require that organizations must have consent up front for any kind of electronic marketing to individuals. "Consent" means some positive indication of consent, which must be freely given and informed. In other words, to constitute "consent," individuals must fully appreciate that they are consenting and fully appreciate what they are consenting to. There is one exception to the rule about having consent up front. It is known as the "soft opt-in."

The "Soft Opt-In"

Under the soft opt-in, organizations are allowed to send direct marketing electronically to *existing* customers (or to recipients with whom the company has negotiated for a sale in the past), *provided*:

- the marketing in question is for similar products or services,
- the target was given a chance to refuse marketing material at the time her details were originally collected, and
- the target has been given an opt-out in each subsequent marketing communication.

What Are Similar Products And Services?

The Information Commissioner is focusing on reasonable expectation in addressing this question, on the basis that the intention is to ensure that individuals do not receive promotional material about products and services which they would not reasonably expect to receive. For example, someone who has shopped on-line at a supermarket's website might reasonably expect at some point in the future to receive further emails promoting the diverse range of goods available at that supermarket. The requirement to offer an opt-out each time promotions are sent is intended to give recipients a simple means of stopping them in future, and the Information Commissioner will be focussing for the time being on failures to comply with opt-out requests.

Rules About Identifying The Sender

The Regulations attempt to prevent the conventional practice by spammers of disguising junk mail with tempting and sometimes irrelevant subject headings, and the practice of disguising their identity by including a dud email address in the "From" field. You now have to make it clear that your unsolicited material is just that – and without the recipient having to open the message to see it. In addition, the spammer must provide the email recipient with a valid address and a simple means by which to unsubscribe. The Advertising Standards Authority, whose reissued Codes of Advertising, Sales Promotion and Direct Marketing incorporate the new rules, has already upheld its first complaint. It was made against a Southampton-based promotions company for sending unsolicited emails without recipients' prior consent.

How Does This Apply To Text, Picture, And Video Messaging?

The short answer is: the new rules apply exactly as they do to email. The practical limitations of standard mobile screens do not mean that marketers can ignore the rules. Assuming the recipient has clearly consented to the receiving of messages, each message must identify the sender and provide a valid suppression address, for example: XYLtdPOBox123SK95AF. If you are relying on the soft opt-in exemption, then there is the additional obligation to provide a simple means of refusing further marketing with every message. For example: 2STOPMSGTXT'STOP'TO[insert 5 digit short code].

Application Of The Regulations

The Regulations sit next to the Data Protection Act 1998, with which everyone must continue to comply. The important point to note,

however, is that whereas the Data Protection Act only applies to marketing using contact information that actually identifies the individual, for purposes of the Regulations, marketers do not need to know individuals' names in order to conduct a direct marketing exercise. Regardless of whether the Data Protection Act applies to the marketing in question, the Regulations *will* apply if the organization is using electronic means to send unsolicited direct marketing.

Importantly, the new rules do not extend to *companies* that receive electronic marketing, so b2b marketers are free to continue as they were, at least for now. The Government took the view that email and text messaging do not impose the real time disturbance and costs that justify corporate rights against phone and fax marketing, both of which have been regulated since 1999. This limitation may be reviewed in the light of the working experience of the new rules.

There is, however, one very striking anomaly in that companies are excluded but partnerships and sole traders are not. The same rules apply to partnerships and sole traders as do to consumers. This is something of a mystery, particularly since the Government recognized the inconsistency, which first appeared in the draft Regulations, when it responded in September to the public consultation. It left it in, saying it might point to further rights for corporates in the longer term.

On its face, it seems sensible that companies should be allowed to market to one another (including via emails to their employees) without undue privacy concerns. It is, of course, still open for companies to put up firewalls to block a good proportion of what they do not want, and for them to participate in the Direct Marketing Association's e-Mail Preference Service, administered by the Direct Marketing Service in the US (see www.dma.org.uk).

So, perhaps, the balance is about right. Nevertheless, the All Party Parliamentary Internet Group has already called for the Department of Trade and Industry to ban the sending of spam to business addresses when it changes the rules on business-to-business cold calling (probably next year), particularly since it is not clear what is business spam and what is not. For example, is an invitation to buy Viagra sent to the sales address of a shipping company, having no obvious business relevance, caught by the Regulations or not? According to the Information Commissioner's recent Guidance, emails to corporations are simply not covered *per se* (except insofar as there is a requirement to identify the sender and to provide contact details), so the email in this example would be lawful.

Cookies

Regardless of whether a cookie collects data which identifies individuals, from December 11, 2003 onward it will be mandatory before installing any cookie to tell the terminal user what its purpose will be, and to allow her to refuse it. In fact, the rules extend to any kind of device or "spyware" that may be installed on a user's terminal via a public telephone network with the object of collecting information about them. This is a significant development and extends the arm of privacy considerably further than the Data Protection Act. There are exceptions for the storage of or access to information required merely to send or enable a communication over a public network or where strictly necessary for providing a service at the user's request.

Location Data

Location data is data that records information about the geographical location of a user's terminal equipment. Location data is increasingly used to enhance targeted marketing, and we will be seeing much greater use of it in the future. Under the Regulations, the use of location data will for the most part be prohibited unless (i) the network operator (such as Vodafone or T-Mobile UK) has given the user or subscriber certain information, including whether the data will be transmitted to a third party service provider, before consent is obtained; (ii) the user or subscriber has given (and not subsequently withdrawn) his consent; and (iii) the user or subscriber is given the opportunity – simply and free of charge – to withdraw consent in respect of *each* connection to the network or *each* transmission.

The Regulations also consolidate existing rules on marketing by fax and telephone, the use of automated calling, and the use by telecom network operators of traffic and billing data. There are also provisions relating to subscriber directories, security, itemized billing, tracing of nuisance calls, and automatic call forwarding.

Conclusion

The Regulations will present significant challenges to organizations that market to individuals or partnerships using email or other electronic media. Marketers clearly need to consider the implications for the future, but also whether mailing lists compiled before December 11, 2003 are still usable (in light of the new consent requirements) and how the new rules may affect the use for marketing of bought in and rented lists.

Every organization with a website also needs to consider whether the new rules for using cookies affects them.

P

(Endnotes)

1 Marcus Turle is a technology lawyer with City of London law firm Field Fisher Waterhouse. He also specialises in privacy and freedom of information matters, covering all aspects of the Data Protection and Freedom of Information Acts in the UK, as well as other related areas such as the regulation of e-marketing. He advises both public and private sector bodies on the operational impact of privacy regulation, and on compliance issues. For information on any of these areas or any of the issues discussed above, please contact the author at marcus.turle@ffw.com.

Privacy Regulation

Spring 2004

The European Commission's First Report on the Implementation of the Data Protection Directive: Towards Greater Convergence?

Jon G. Filipek[1]
Weil, Gotshal & Manges LLP
Brussels, Belgium
jon.filipek@weil.com

Broadly satisfactory, though in need of improved implementation and consistent application and interpretation – that is the broad assessment reached by the European Commission in its "First Report on the implementation of the Data Protection Directive (95/46/EC)" (the "Report"),[2] following a comprehensive review of the legislation, adopted some eight years ago this October. As discussed in further detail below, headline conclusions emanating from the Report include the following:

- First, there will be no amendments to Directive 95/46 (the "Directive").[3] The Commission – which has the exclusive power of legislative initiative in this area — does not plan to propose any, at least in the near term. A great volume and variety of criticisms were raised in the course of the review, but these, in the Commission's view, are either misplaced or can be dealt with by means other than EU-level legislative change.

- Second, the Commission identifies divergent implementation of the Directive by the Member States as the central problem area warranting attention and rectification. Rather than proposing amendments, the Commission sets forth an ambitious Work Programme for 2003-2004 aimed at reducing divergence by other means. In brief, where divergence is the result of "incorrect" or "incomplete" implementation, the Commission intends to prod the Member States concerned – by persuasion if possible, by litigation if necessary – to rectify the situation. Where divergence represents "correct

implementation" within the Directive's "margin of manoeuvre," but imposes unwarranted costs on operators, the Commission will seek to arrive at uniform interpretations of the Directive's requirements via dialogue with the Member States and national supervisory authorities.

- Third, in the Commission's assessment, compliance with Directive generally has been "very patchy," given the reluctance of companies to conform their practices to complex and burdensome rules when "the risks of getting caught seem low." Relatedly, the Commission concludes that enforcement is not a priority for the national authorities, which lack sufficient funding, and that data subjects have an "apparently low level of knowledge" of their rights under data protection law.

- Fourth, the Commission singles out "harmonious application of the rules relating to the transfer of data to third countries" as a "priority" area of concern. The Commission's Work Programme sets forth a number of action items to facilitate extra-EU transfers of personal data, including further determinations on third-country adequacy and further "standard contractual clauses" for transfers to countries not subject to a formal adequacy determination. The Commission also intends to give focused consideration to the role of so-called "binding intra-corporate rules" in ensuring adequate protection for transfers of personal data among group companies operating in multiple jursidictions inside and outside of the EU. Of particular interest is the Commission's pointed criticism of the practice – presently followed, it appears, by the great majority of Member States – of permitting organizations to "self-assess" the adequacy of protection in third countries not subject to a formal adequacy determination, and to transfer personal data to such countries on the basis of a positive self-assessment. Although it is unclear, the Report raises the question whether the Commission will take near-term action to pressure Member States to terminate this practice.

This Article discusses the Report's findings in greater detail below, focussing in particular on divergent Member State implementation and how the Commission intends to address the problem. Before turning to the Report, this Article provides as background a quick overview of the Directive and its history.

Background

The Directive was adopted on October 24, 1995 following more than five years of consideration by the Community institutions – an extraordinarily long legislative procedure period by any reckoning.[4] Implementation of the Directive proved equally tortuous. Although the Member States were called upon to transpose the Directive's requirements into their national legal systems within three years – *i.e.*, by October 25, 1998 – only four Member States met the deadline.[5] Ultimately, in December 1999 the Commission saw fit to bring five Member States – France, Germany, Ireland, Luxembourg, and the Netherlands – before the European Court of Justice for failure to notify implementing measures.[6] Even as of this writing – some five years after the deadline – Ireland has only recently completed implementation of the Directive (though it has not yet notified the relevant measures to the Commission), and France still has not fully implemented.[7]

The Report is mandated under Article 33 of the Directive, which requires the Commission to report "at regular intervals" on the "implementation of this Directive," providing "if necessary, suitable proposals for amendments." As part of this effort, the Commission is also specifically charged with examining "the application of this Directive to the data processing of sound and image data relating to natural persons." The deadline for implementation of the Directive was October 25, 1998, and thus the Report was in principle due by October 25, 2001. However, the Commission issued the Report some 18 months late, on May 15, 2003, citing substantial (and continuing) Member State tardiness in implementing the Directive as the reason for the delay.

The Directive in a Nutshell

The Directive applies to the "processing" (defined as broadly as possible to include even mere "consultation" or "use") of "personal data" (relating to an identified or identifiable natural personal, called a "data subject") – whether by "automatic means" (*i.e.*, electronic or computer-based data), or otherwise in connection with a structured, paper-based "filing system." (*See* Articles 2(a)-(c) & 3). The Directive is a horizontal measure, applicable to all sectors of activity, with two broad exceptions: (i) processing carried out for purely "personal" or "household" activities; and (ii) processing in the course of so-called "third-pillar" activities by the State, such as public security, defense, State security and criminal law matters. (*See* Article 3(2)).

All processing falling within the Directive must in principle comply with the following key requirements:

1. **Notification/Registration** (Articles 18 & 19) - Persons engaged in the "automatic" processing of personal data generally must register with the relevant national regulator(s).

2. **"Legitimate Processing Criteria"** (Articles 7 & 8) - Processing is prohibited unless it falls within a specified criteria (*e.g.*, "unambiguous" consent, controller's "legitimate interests"). For sensitive data (*e.g.*, health, race/ethnicity, religion, "sex life"), stricter criteria apply (*e.g.,* "explicit" consent).

3. **Data Quality Principles** (Article 6) - Personal data must be processed in conformity with certain principles – *e.g.,* data be "fairly and lawfully" processed and "kept up to date.")

4. **Information Requirements/Notice to Data Subjects** (Articles 10 & 11) - Data subjects must be given certain core notice elements (*i.e.*, the identity of the data controller and the purposes of processing) plus any "further information" necessary to guarantee "fair processing."

5. **Third-Country Transfers** (Articles 25 & 26) - Extra-EU transfers are prohibited unless: (i) subject to "adequate protection"; (ii) an exemption applies (*e.g.*, consent); (iii) made pursuant to approved safeguards; or (iv) individually authorized by the regulator.

6. **Data Subject Rights** (Articles 12, 14 & 15) – Data subjects must be given rights, (*e.g.*, to access and correct personal data, to object to direct marketing).

7. **Security** (Article 17) - "Appropriate" technical and organizational measures must be taken to protect personal data against unauthorized or unlawful processing (*e.g.,* hacking).

Member States must provide for sanctions (*e.g.,* criminal penalties) and compensation to data subjects (*e.g.*, civil claims for "unfair processing") in the case of infringements of the Directive's requirements. (Articles 22-24).

Compliance with the Directive is incumbent upon the data "controller," which is the natural or legal person who determines the purposes and the means of the processing of personal data. (Article 2(d)). Under the Directive's applicable law provisions, a Member State is required to apply its national law (as harmonized by the Directive) to the processing of personal data where:

- the processing is carried out "in the context of" (*i.e.*, for the purposes of) an establishment of the controller on the terri-

tory that Member State (the "establishment criterion" of Article 4(1)(a)); or

- the controller is not established anywhere in the EU but "makes use of equipment" situated on the territory of that Member State (the "technical means" criterion of Article 4(1)(c)).[8]

Notably, where a controller has establishments in multiple Member States, the controller must "ensure that each of these establishments complies with . . . the national law applicable." (Article 4(1)(a)). By way of example, for a controller incorporated in the United Kingdom with an unincorporated branch in Spain, in principle U.K. law will apply to processing related to the U.K. operations and Spanish law will apply to processing related to the Spanish operations.

In theory, the application of different Member State laws to the same controller should not be overly problematic: the Directive is intended to harmonize national laws, and therefore compliance requirements should be similar regardless of the national law applied. The Directive, however, like all directives, is binding on Member States "as to the result to be achieved" but leaves to the Member States a margin of manoeuvre as to "the choice of form and methods." (EC Treaty, Article 249). In practice, numerous and substantial divergences exist in the ways Member States have chosen to implement the Directive, as the Report amply demonstrates.

The Commission's Report – Main Conclusions

The Report consists of two documents – the Report itself, which sets forth the Commission's conclusions, and an *Analysis and Impact Study on the Implementation of Directive EC 95/46 in Member States* (the "Impact Study"),[9] which broadly assesses the impact of the Directive's implementation on the Internal Market. Further, in connection with its review, the Commission commissioned two professional studies from independent experts: a *Comparative Summary of National Laws* (the "Comparative Summary"), a document of more than 200 pages reviewing Member State implementation of the Directive; and *The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data.*[10] The Report results from an admirably open and inclusive consultation process involving governments, businesses, and other institutions, consumer associations, and the general public.[11] A wealth of detailed information on national transposition of the Directive is supplied in the Report and its accompanying documents. These should serve as a useful, initial reference for practitioners seeking to determine how particular Member States have implemented particular provisions of the Directive.

The overarching conclusion of the Report is that, despite delays and gaps in Member State implementation, the Directive in its first five years of operation has largely been a success. The Commission states that the Directive "has fulfilled it principal objective of removing barriers to free movement of personal data between Member States," citing the absence of any reported cases where "the transfer of personal data between member States has been blocked or refused on data protection grounds."[12] In addition, the Commission concludes that the Directive has achieved its corollary goal of achieving a high level of data protection.[13] The Commission notes, however, that Internal Market policy objectives extend beyond "mere free movement" and include the encouragement of cross-border activity within the EU and the simplification of the regulatory environment in which businesses operate. "Judged against these criteria," the Commission concludes, "the divergences that still mark the data protection legislation of the Member States are too great," and "stakeholders are right to demand more convergence in legislation and the way it is applied."[14]

Nevertheless, the Commission concludes that the "results of the review on balance militate against proposing modifications to the Directive at this stage," given that experience with implementation of the Directive is limited (most Member States only implemented in 2000 -2001), many of the difficulties identified can be rectified by other means, and many of the legislative changes sought by commentators in the review process would entail a reduction in the level of data protection, which is not warranted.[15] Rather than offering specific amendments at this time, the Commission has instead proposed a Work Programme for 2002-2003 aimed at reducing divergent implementation of the Directive. The Commission's Work Programme is discussed further below.

Another general issue warranting attention, in the Commission's view, is the level of compliance with the data protection rules and, relatedly, enforcement of the rules by the authorities. While acknowledging the difficulty of obtaining information on these matters, the Commission states that anecdotal evidence, as well as some hard information, "suggests the presence of three interrelated phenomena":

- under-resourced national authorities, which give low priority to enforcement action;
- "[v]ery patchy compliance" by data controllers, which are reluctant to change existing practices to conform with complex and burdensome rules, in particular when "the risks of getting caught seem low"; and
- an "apparently low level of knowledge" of data subjects of their rights under the data protection law.[16]

Finally, as regards the processing of sound and image data, the Commission generally concludes that such processing "falls within the scope of all national laws implementing the Directive and . . . the application of the Directive to these categories of processing has not been particularly problematic."[17]

The Problem of Divergent Implementation

The Report identifies divergences in Member State implementation of the Directive as the central problem warranting attention and rectification. To illustrate the difficulties such divergences present to multi-jurisdictional operators, consider the example of a group of companies operating in multiple Member States which decide to outsource certain ongoing activities to a processor in a third country. As the starting point, it must be emphasized that all processing operations falling within the Directive's scope must comply in principle with all the key compliance requirements discussed above,[18] to the extent applicable. Thus, with respect to the transfers of personal data involved in the outsourcing, it must be considered, among other things:

- whether an appropriate basis for the transfers exists under the Directive's third-country transfer regime – *i.e.*, adequate protection or an exemption, such as consent (Articles 25 & 26);
- whether the transfers need to be reflected in the controller's data protection registration, assuming registration is required (Articles 18 & 19);
- whether customers must be provided with notice (and when and in what form) of the transfers (Articles 10 & 11); and
- whether any particular information security requirements apply to the transfers (Article 17).

Accordingly, the contemplated outsourcing operation may implicate at least four separate compliance requirements under the Directive. For a group with companies in ten EU Member States, the decision to outsource may therefore entail a review of the position on at least 40 discrete clusters of issues. Further, in order to determine the position in particular jurisdictions, it may be necessary to consult not only the data protection statute itself but various secondary laws, case law (concerning civil claims and appeals from decisions of the national supervisory authority), legal guidance and advice from the supervisory authority, as well as the supervisory authority's enforcement policy and practice, as set forth in the authority's annual reports.

The great bulk of the Report and its accompanying documents is devoted towards identifying the most problematic areas of diver-

gent implementation. These are highlighted in the Report itself, further addressed in the *Impact Study*, and then elaborated in great detail in the 204-page *Comparative Summary.* Though a comprehensive review of these findings is well beyond the scope of this article, the following examples of divergent implementation should provide a sense of the serious difficulties facing organizations attempting to comply with data protection requirements on a pan-European basis.

"Legitimate Processing Criteria" (Articles 7 & 8).[19] As the Report observes, the Directive's legitimate processing criteria form the "core" of the Directive, and yet divergent Member State implementation of these provisions presents a "particular impediment to a harmonised framework and creates problems for businesses operating on a multinational scale."[20] This is illustrated by national implementation of what are arguably the two most important criteria – Article 7(a), which permits processing undertaken on the basis of the data subject's "unambiguous" consent, and Article 7(f), which permits processing carried out in the controller's "legitimate interests," provided such interests are not overweighed by the privacy rights and interests of the data subject. In the United Kingdom, for example, the law implementing Article 7(a) simply identifies "consent" as a criterion for processing – without the qualifier "unambiguous" – and the regulator's guidance indicates that consent in some cases may be implied. By contrast, in Italy, data subject consent must in principle be in writing in order for this criterion to apply.

Member State implementation of Article 7(f)'s critically-important "legitimate interests" balancing test – which serves as a fall-back justification of sorts for processing when other criteria are not available – is even more inconsistent: some Member States simply repeat the language of the Directive; others import additional requirements by reference to secondary legislation (which in many instances has not yet been adopted); and others have implemented the test so as to tilt the balance sharply in favor of the data subject.

Information Requirements/Notice to Data Subjects (Articles 10 & 11).[21] The Report finds that Member State implementation of the Directive's notice provisions also varies "very considerably."[22] Thus, for example, while all Member States generally require provision of the two core notice elements set forth in the Directive – *i.e.*, the identity of the controller and purposes of the processing – some, such as the United Kingdom, qualify the obligation by adding that the information should be provided ("or made readily available") "so far as practicable." Further, a number of Member States require that some or all of the "additional information" requirements identified in the Directive – *e.g.*, recipients of personal data, information on data subject rights – must *always* be provided

to data subjects (*e.g.*, France, Finland, Germany), or must be provided *unless* the information is *not* necessary to ensure fair processing (Belgium). The Directive, by contrast, requires the provision of such additional information requirements only if "necessary" to ensure fair processing. Such divergences make the development of coherent pan-European notices for customer documentation very difficult.

Notification/Registration (Articles 18 & 19).[23] All of the Member States provide in principle for notification to the national data protection authority of automatic (*i.e.*, computer-based) processing of personal data, subject in some Member States to the appointment of a data protection officer in lieu of notification. However, some Member States also in principle require the notification of manual (*i.e.*, paper-based) processing of personal data (*e.g.*, Denmark, Greece, Italy, and Luxembourg), or at least certain kinds of manual processing (*e.g.*, in Portugal, manual processing of sensitive data; and in Finland, manual processing involving third-country transfers of data or certain automated decision-making). The Member States have also made fairly wide use of exemptions from notification, as sanctioned by the Directive, typically for certain standard processing operations – for example, salary administration – provided that the operations are consistent with rules and conditions specified by the Member States. Although some standard exemptions tend to be similar across the EU, there is substantial variation among Member States in respect of the precise rules and conditions for applicability. Finally, the Directive permits the appointment of a data protection officer in lieu of notification, a concept which originated in Germany prior to adoption of the Directive and has been continued there. Although some other Member States (*e.g.*, Luxembourg and Sweden) provide for this possibility, the concept has not been fully developed, and the majority of Member States make no provision at all for this alternation to notification.

Third-Country Transfers (Articles 25 & 26).[24] The Report finds "very broad" divergences in Member State implementation of the Directive's international transfer regime.[25] Differences include the precise conditions for application of Article 26's derogations (permitting transfer to third countries which do not provide for adequate protection) as well as a variety of smaller points – for example, whether non-EU members of the European Economic Area (*i.e.*, Norway, Iceland, and Lichtenstein, which are obligated to implement the Directive) should be treated as equivalent to EU Member States for purposes of data transfers to those countries.

More generally, the Report identifies fundamental differences in the degree of control exercised by the Member States and national supervisory authorities over third-country transfers of personal data. For example, some Member States require authorization of all third-

country transfers, including even those which fall squarely within one of Article 26's derogations, an approach the Commission considers to be inconsistent with the system of control envisioned in the Directive. The key divergence, however, concerns Member State treatment of transfers to third countries that have not yet been the subject of a formal determination of adequate protection at the EU or the national level. This issue is key since, to date, only five such determinations have been made (*i.e.*, with respect to Hungary, Switzerland, Argentina, the U.S. "safe harbor" arrangement, and the Canadian Personal Information Protection and Electronic Documents Act). Accordingly, a critical question faced by the national supervisory authorities has been whether controllers may themselves assess whether protection is adequate in the contemplated country of transfer, in the absence of a formal adequacy determination. On this crucial point the Member States fall into three basic camps:

- The legislation in four Member States (Austria, Greece, Portugal, and Spain) makes clear that, unless and until a formal determination of adequacy has been made, a transfer of personal data to a third country is prohibited unless the transfer falls within one of the Articles 26's derogations.

- The position is unclear in two Member States – Italy (where transfers must be notified to the regulator, which may then raise objections) and Belgium (where legislation relevant to the issue is not yet complete).

- In the remaining nine jurisdictions, however, the position appears to be that, in the absence of an adequacy determination for a particular country, controllers may themselves determine whether protection is adequate in, and on that basis transfer personal data to, the country concerned.

Addressing Divergent Implementation – The Commission's Work Programme

In its review, three basic approaches to addressing divergent implementation were available to the Commission. A number of commentators, for example, called for replacing the Directive's existing jurisdictional scheme with what is variously called a "country of origin," "lead regulator," or "single passport" approach. Although the proposals differ somewhat, the unifying concept is that:

> [t]he Directive should be amended to make clear that there is no need to comply with legislation in multiple jurisdictions. The solution is to allow the data controller discretion to adopt a 'country of origin'

> approach so that the compliance with the rules of the lead regulator is only required.[26]

The country of origin approach would not reduce divergent implementation, but would greatly facilitate compliance by making multi-jurisdictional operators subject to the rules of one Member State only.

Alternatively, the Commission could have proposed specific amendments aimed at reducing the Member States' "margin of manoeuvre" in implementation. Under this approach, multi-jurisdictional operators would remain subject to the law of multiple Member States, but compliance requirements in the different jurisdictions would be more similar it is now. As noted, the Commission has declined to propose any revisions to the Directive noting, among other things, that "the ambition of the Directive is approximation and not complete uniformity."[27]

In the Commission's view, the divergences identified in its review "have different causes and different consequences," and therefore require "a range of different solutions."[28] In particular, certain divergences arise from "incorrect" or "incomplete" implementation of the Directive; cited as examples are the Directive's provisions on legitimate processing criteria (Article 7), sensitive data (Article 8.1), notice to data subjects (Article 10), and the derogations from the requirement of adequate third country protection. (Article 26).[29] Where Member State implementation amounts to non-compliance with Community law, the Commission intends to persuade Member States to bring their national laws into conformity with the Directive – if possible, through persuasion, or, if necessary, by infringement litigation before European Court of Justice.

Other divergences, however, may represent "the legitimate result of correct implementation . . . within the margin of manoeuvre allowed by the Directive;" cited as examples are the Directive's provisions on notification (Articles 18 and 19) and international transfers (Articles 25 and 26). [30] Where such cases pose present "significant negative consequences in the Internal Market" or create "unjustified administrative burdens for operators," the Commission intends to pursue more uniform implementation through discussions with, and greater coordination among, the Member State and national supervisory authorities. Should persuasion and coordination fail to result in more uniform interpretations of the Directive's requirements, the Commission may later propose amendments to the Directive to force uniformity.

To this end, the Report sets forth a "Work Programme for a Better Implementation of the Data Protection Directive (2003-2004)"[31] con-

sisting of ten action items for the Commission, the Member States and the national supervisory authorities, and the so-called "Article 29 Working Party," an advisory group established pursuant to Article 29 of the Directive and consisting of representatives of the Member State national supervisory authorities and of the Commission. Key action points include:

- Bilateral discussions carried out by the Commission with the Member States and the national supervisory authorities concerning changes needed to bring national legislation into full alignment with the Directive;

- Commission action, including infringement litigation if necessary, to improve Member State notification of legal acts implementing the Directive and of national authorizations of international data transfers granted under Article 26(2) of the Directive;

- Discussions within the Article 29 Working Party on better enforcement, including the exchange of best practices and, possibly, EU-level sectoral investigations aimed at developing information on implementation and recommendations for securing improved compliance;

- Proposals by the Article 29 Working Party (or the Commission, if the Working Party is incapable) for simplification of Member State notification/registration requirements and for a co-operative mechanism to facilitate notifications/registrations by multi-jurisdictional operators; and

- Proposals by the Article 29 Working Party for a more uniform interpretation of Article 10's notice requirements.

In addition, the Work Programme sets forth a series of actions to improve operation of the Directive's third-country transfer regime, which the Commission considers a "priority" item. These include discussions with the Member States on bringing infringing national measures into conformity with the Directive and input from the Article 29 Working Party on the simplification and approximation of the conditions for data transfers. In addition, the Report makes clear that the Commission intends to make more extensive use of the Commission's powers under the Directive to adopt measures facilitating international transfers, including further adequacy determinations on third-country adequacy; further "standard contractual clauses" pursuant to which transfers may be made to countries not subject to a determination of adequacy; and further consideration of the role of so-called "binding intra-corporate rules" for the transfer of personal data among group companies operating inside and outside of the EU.

Concluding Remarks

The reluctance of the Commission to propose any amendments to the Directive, at this juncture, is somewhat disappointing. While an overhaul of the Directive along the lines of the "country of origin" principle was never a politically realistic objective, specific amendments aimed at reducing divergences in implementation or addressing certain of the Directive's more obvious deficiencies would have seemed to be in order.

For example, the general (though not uniform) consensus seems to be that the notification requirement, presently implemented in widely varying fashion by the Member States, serves little protective purpose while requiring substantial resources both of businesses and national supervisory authorities. The Commission acknowledges this, yet regrettably it declined to propose bold action to address the situation – for instance, replacement of the existing notification requirement by a system requiring notification of only a limited range of clearly problematic data processing activities (*e.g.*, data-mining), backed up by the right of data subjects, exercisable under existing Article 12, to obtain from any controller information concerning personal data being processed about them. As a further example, the Directive's legitimate processing criteria could also have benefited from amendment at the EU level – for example, mandatory language clarifying that data subject "consent" need not always be in writing in order to fulfill Article 7(a). Similarly, the Commission recognizes that the applicable law provisions of Article 4(1)(c) – pursuant to which a Member State must apply its national law to processing by controllers not established in the EU but which "make use of equipment" situated in that Member State – "may not be easy to operate and . . . [need] further clarification."[32] While the Commission states that it may "in due course" find it necessary to propose amendments to these provisions, its call for "more experience" before doing so seems unduly cautious given the urgent need to clarify the Directive's uncertain application to non-EU, Internet-based processing of personal data.

That said, any critique of the Report must acknowledge the extremely difficult task the Commission faced in weighing and reconciling the views of many parties with varying, sometimes opposing, interests. The Commission's decision not to propose amendments at this time also must be considered against the political realities. The extraordinarily lengthy legislative process preceding the Directive's adoption in 1995 suggests that any revision of the Directive would not be speedy. Further, as one commentator has noted, "any proposed amendments, even if justified in substance, could open a Pandora's box by encouraging the European Parliament to propose further amendments even stricter than the Directive."[33] Accordingly, there

is merit in the Commission's comment that its plan to rely on persuasion and coordination to overcome divergence may produce results "more quickly than would an amendment of the Directive and so should be fully exploited first."[34]

Further, the Commission's expressed intention to rectify "incorrect" transposition of the Directive – through persuasion if possible but through litigation if necessary – is welcome and should serve to reduce divergences in Member State implementation. Whether divergent but "correct" (*i.e.*, within the Directive's "margin of manoeuvre") implementation may be successfully addressed through persuasion and coordination, as the Commission intends, is far less clear. For example, the Commission has called upon the Article 29 Working Party to assist the Commission and the Member States in arriving at "uniform interpretations" of the Directive's contested provisions. However, the Working Party has already produced a vast corpus of interpretative guidance over the past five years, and this work does not seem to have reduced divergence to an appreciable degree. Further, in its guidance to date, the Working Party has tended to take a maximalist approach to data protection, and any "uniform interpretations" issued by the Working Party may well reflect a highest-common-denominator mindset. In any event, it is to be hoped that the Commission will make good on its threat to propose amendments to the Directive if persuasion and closer coordination fails to reduce the negative impacts of divergent Member State implementation.

In closing, a few comments are warranted concerning the Directive's regime for international data transfers, given its critical importance to multi-national businesses operating in the EU. First, by and large, the Commission's objectives in this area are positive. For instance, the Commission apparently intends to take action to end the practice of some Member States to require authorization of all third country transfers – even those which fall within one of Article 26's derogations. Also welcome is the Commission's expressed intention to make greater use of its powers under the Directive to adopt measures facilitating extra-EU transfers of personal data. These include further third-country adequacy determinations, and further "standard contractual clauses." The Commission also apparently intends to give focused consideration to the role of so-called "binding intra-corporate rules" for the transfer of personal data among group companies operating in multiple jurisdictions inside and outside of the EU. This idea has been floated for years; a formal decision identifying appropriate safeguards for such transfers could prove extremely useful for international groups operating in the EU.

Second, the Commission states that the available evidence "suggests that many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection,"

and "[y]et there is little or no sign of enforcement actions by the supervisory authorities."[35] Of particular interest are the Commission's remarks concerning the "lax" approach adopted by some Member States, "where the assessment of third country adequacy is supposed to be made by the data controller, with very limited control of the data flows by the Member State or the national supervisory authority."[36] In the Commission's view, this approach "does not seem to meet the requirement . . . of Article 25(1)," which obliges Member States to ensure that transfer to third countries "may only take place if . . . the country in question ensures an adequate level of protection." As noted above, the Impact Study indicates that nine Member States follow this "lax" approach.[37] Thus, in the Commission's view the great majority of Member States are presently applying the central provision of the Directive's transfer regime incorrectly, thus raising the question whether the Commission will take action to pressure these "lax" Member States to tighten controls, so that transfers may be made on the basis of Article 25(1) only if the third country is the subject of a formal adequacy determination at the EU or national level.

Such action would be regrettable. It seems fair to say that the "lax" approach adopted by the majority of Member States has, in fact, enabled the Directive's transfer regime to function during its first five years without crippling international data flows out of the EU. Permitting controllers themselves to assess third-country adequacy prior to the issuance of a formal adequacy determination is fully consistent with the express language of Article 25, and the approach does not necessarily involve an abandonment of regulatory control.[38] In any case, the continuing viability of controller self-assessments of adequacy is a key issue, and practitioners would be well advised to follow the Commission's action in this regard.

P

(Endnotes)

[1] Jon G. Filipek is a partner in the Brussels office of Weil, Gotshal & Manges LLP. He has extensive experience with the Data Protection Directive and other EU privacy legislation, and has counseled clients on compliance with data protection requirements in upwards of 20 European jurisdictions.

[2] *Report from the Commission: First report on the implementation of the Data Protection Directive (95/46/EC),* COM(2003) 265 final; and Commission Press Release, *Data protection: Commission report shows that EU law is achieving its main aims,* IP/03/697 (May 16, 2003), (the "Press Release"), available at: http://www.europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_en.htm.

[3] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the protection of personal data and on the free movement of such data, O.J. L281/31 (November 23, 1995).

[4] The Commission's original proposal for a general data protection directive was tabled on July 27, 1990. *See* Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM(90) 314 final – SYN 287, O.J. C277/3, November 5, 1990.

[5] Directive, Art. 32(1); Press Release, at para. 7.

[6] For further details concerning the litigation against the Member States, see the Report, at 3, n.1.

[7] *See* European Commission, *Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data*, available at: http://www.europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm

[8] A third, and more obscure, basis for application of national law is where the "controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law." Directive, Art. 4(1)(b).

[9] The Impact Study, like the Report, is available at: http://www.europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_en.htm.

[10] D. Korff, *Comparative Summary of National Laws* (Study Contract ETD/2001/B5-3001/A/49), September 2002; and British Institute of International & Comparative Law, *The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data* (Service Contract CNS/2002/AO-7002/A/55). The two studies are available at: http://www.europa.eu.int/comm/internal_market/privacy/studies_en.htm.

[11] In addition to seeking input from the Member State governments and national supervisory authorities, the Commission solicited comments from the general public via an invitation the Official Journal of the European Communities (resulting in 73 "high quality" position papers); posted two online questionnaires, one for data controllers and another directed to data subjects (garnering more than 10,000 responses); and held a two-day conference in Brussels on September 30/October 1, 2002 (attended by more than 400 interested parties). *See* Press Release.

[12] Report, at 10.

[13] *Id.*

[14] Report, at 11.

[15] Report, at 7-8.

[16] Report, at 12-13.

[17] Report, at 20-21.

[18] *See* discussion in "The Directive in a Nutshell," *supra.*

[19] *See* Report, at 17, Impact Study, at 10-11, and Comparative Summary, at 73-80.

[20] Impact Study, at 44.

[21] *See* Report, at 17-18, Impact Study, at 19-20, and Comparative Summary, at 98-104.

[22] Impact Study, at 19.

[23] *See* Report, at 18, Impact Study, at 26-29, and Comparative Summary, at 167-78.

[24] *See* Report, at 18-19, Impact Study, at 31-35, and Comparative Summary, at 182-95.

[25] Report, at 18.

[26] Comments of the Confederation of British Industries, at 1.

[27] Report, at 11.

[28] *Id.*

[29] *Id.*

[30] Report, at 11 -12.

[31] Report, at 22-26.

[32] Report, at 17.

[33] C. Kuner, "The Commission's First Report on Implementation of the EU Data Protection Directive," World Data Protection Report, at 10 (BNA).

[34] Report, at 7.

[35] Report, at 19.

[36] Report, at 18.

[37] *See supra* n. 24 and accompanying text. The nine "lax" Member States are Denmark, Finland, France, Germany, Ireland, Luxembourg, the Netherlands, Sweden, and the United Kingdom.

[38] For example, in the United Kingdom (one of the so-called "lax" jurisdictions), controllers remain "on the hook" for their adequacy self-assessments. Briefly, according to guidance issued by the national supervisory authority, transfers under Article 25(1) may permissibly be made to countries which have not been the subject of a positive adequacy determination, provided that the controller first determines whether, and takes steps to ensure that, adequate protection of the transferred data exists in the country of transfer. *See* Office of the U.K. Information Commissioner, *Data Protection Act 1998: The Eighth Data Protection Principle and Transborder Dataflows.* However, should a controversy later arise, the supervisory authority (or a court) may conclude that the transfer was not, in fact, subject to adequate protection, and therefore contrary to the law. In the event, controllers which have made erroneous assessments of adequacy may find themselves subject to an order to terminate the transfers, penalties (if the order is disregarded), and damages (in civil litigation).

Privacy Regulation

Spring 2004

Broadband Security:

Developing Legal Standards for a Brave New World

Leslie F. Spasser[1]
Willcox & Savage, P.C.
Norfolk, Virginia
lspasser@wilsav.com

In the spring of 1999, broadband service was still in its infancy. A cable high speed Internet subscriber, self-dubbed "Mr. Nasty," issued a mass e-mail to other subscribers railing against the dangers of broadband service. Using R-rated language and scatological metaphors, he expressed dismay at the fact that broadband gave rise to security concerns that had not been present in the narrowband, dial-up world. Mr. Nasty capped off his observations with the all too vivid analogy that a computer attached to a cable modem was as vulnerable as "a virgin lying naked in a football field on homecoming day."[2]

Notwithstanding the fact that Mr. Nasty could have found a more constructive way to make his point, the validity of the issue that he raised has been borne out over time. By virtue of their inherent structure and their integration with the Internet, broadband services of all types give rise to security issues that did not exist either at all or to the same extent in the narrowband environment. Hand in hand with the benefits and innovations spurred by broadband are potential vulnerabilities that can impact consumers of these new services by exposing them to attacks, information theft, and unwanted intrusion. Providers, in turn, could be exposed to liability arising from these security breaches.

This article explores three questions: (a) In an inherently insecure environment, what level of security are providers legally obligated to offer their customers?; (b) Do broadband providers have a legal obligation to cure, mitigate, or inform their customers of security vulnerabilities?; (c) What practical steps should broadband providers take to minimize liability for security problems inherent in the technology upon which their services are based?

These questions are posed in a legal environment that is murky at best. Existing laws governing Internet security tend to apply to specific industries (such as the Health Insurance Portability and Accountability Act to the health care industry, and Gramm-Leach-Bliley Act to the financial services industry) rather than to online businesses in general, and focus upon the secure maintenance of customer information to a greater degree than the provision of secure services.[3] Nonetheless, the standards being created by these regulations impact the direction in which the law is evolving in the area of service security.

On the enforcement front, the FTC has addressed security issues recently in the context of consent decrees involving Microsoft Corp., Eli Lilly and Company, and Guess? Inc.[4] While the FTC's focus has been on alleged misrepresentations about the level of security provided by these companies' websites or products, the consent decrees set forth requirements that may form the foundation for more widely applicable standards for responsible security practices.

To date, no court has found that Internet service providers owe their subscribers a common law duty of care to ensure the security of their services. However, a recent lawsuit filed against Microsoft in California [5] arising out of damage allegedly caused by security holes in the Windows operating system bears discussion because the outcome could set precedent regarding the security obligations of other types of software and service providers.

Overlaid on the legal framework are evolving industry standards for broadband security, wireless security, and general Internet security. To the extent that a legal duty of care exists, these industry standards are likely to play an increasingly important role in defining minimum "reasonable" steps a broadband provider should take in order to protect its customers and its services.

In this shifting environment, broadband providers can mitigate security risks for their customers and liability for themselves by taking a three-pronged approach that includes (1) the establishment of a security program; (2) the provision of notice to consumers of risks and potential solutions, and (3) the use of contractual safeguards against liability for damage arising out of security breaches. This approach should enable broadband companies to address security in a flexible manner, implement new standards as they become available, and educate their customers on how to help themselves as new threats emerge.

I. Broadband Technology: Opportunities Beget Risk

The hallmarks of broadband service[66] are (a) high speed transmissions[7] and (b) "always on" capability (which means that when the computer

is turned on, it is connected to the Internet and is capable of sending and receiving data).[8] These features enable providers to offer customers multiple services and enable customers to access content quickly, download large files, view streaming video and audio content, and use other speed-dependent services, such as voice-over Internet Protocol ("VOIP"). The deployment of broadband services has jump-started the adoption of new applications, such as wireline and wireless home networking (which enables subscribers to move downloaded content around the home). Other broadband-enabled services in early stages of testing or deployment include broadband home security service, energy management, medical/out-patient monitoring and care, and the networking of household appliances (imagine having the ability to send a signal from your PDA instructing your oven to begin preheating as you are on your way home from work).

Broadband service has changed the way consumers use technology and has the potential to spur continued innovation that will benefit consumers. Yet the very qualities that make broadband so desirable also create or exacerbate security risks inherent in networked services - risks that will only increase as more devices within the home are connected to the broadband network. For instance, the increased speed of the broadband connection can enable hostile programs such as Trojan Horse or back-door programs[9] to be installed without the customer experiencing a noticeable deterioration in the speed of service during the installation process. The "always on" characteristic increases the vulnerability of a customer's computer to attack because as long as it is turned on, it is a fixed target, accessible from the Internet, and visible to potential intruders.[10]

Broadband-enabled services, such as home networking also create increased security risks. The more reliant consumers become on these services and the more devices they attach to their networks, the greater the potential harm in the event of a security breach. Although we have not yet reached the point where a disgruntled neighbor can stage a denial of service attack against the toaster oven next door, the prospect of malicious parties gaining unauthorized access to the video content stored in a consumer's home media gateway is not so farfetched.[11] As with any network, if a broadband-enabled network is compromised, it is possible for an intruder to steal personal information, alter information on attached devices, and otherwise cause havoc to hardware and software. Wireless networks, which have gained increasing popularity for residential and business use, are notoriously insecure.[12] These flaws can be mitigated somewhat by enabling existing encryption standards, but available solutions are far from foolproof.[13] In addition to eavesdropping, the vulnerabilities in wireless networks can allow unauthorized devices to connect to a consumer's network, third parties to hijack existing sessions, and allow third parties to engage in denial of service attacks.[14]

The challenges presented to broadband providers will grow as they deploy services like VOIP, energy management, and home medical treatment. The extension of the security vulnerabilities of the Internet to IP-based voice communications may be inevitable;[15] however, consumers accustomed to the relatively assured privacy of their telephone calls may be unpleasantly surprised unless these vulnerabilities are clearly identified to them by broadband providers and, to the extent possible, mitigated. Home medical treatment services being developed contemplate providing automatic transmission of vital information (*i.e.*, weight or blood pressure information) from the home to a treatment center via networked medical equipment and remote interaction with doctors or other medical staff. The information transmitted not only is sensitive in and of itself, but by contracting with medical facilities to transmit it, it is likely that broadband providers will subject themselves to the privacy and security requirements set forth in HIPAA.[16]

Finally, security issues facing broadband providers will become more complex as consumers gain the ability to purchase third-party devices and attach them directly to broadband networks without involving the broadband provider at all. While the availability of "plug and play" devices advances the policy goal of enhancing consumer choice and stimulating innovation and competition, a by-product of this openness is the diminution of a provider's visibility into the devices on its network and a compromise of its ability to assure security. Not only does the possibility of authentication failures create a scenario where unauthorized devices might become resident on the network, but if consumers improperly configure their devices, fail to change default passwords to more secure passwords, or fail to take reasonable measure to protect their own equipment and home networks (*i.e.*, installing firewalls and using anti-virus software), then consumer networks could be compromised and unwittingly become relay points for malicious attacks.

The development of broadband-enabled technology and services creates extraordinary opportunities for consumers and broadband providers alike. The security challenges that these otherwise positive developments pose will require broadband providers to develop strategies for assessing security risks and implementing programs to address them.

II. The Evolving Legal Environment

Broadband spans diverse industries and involves a host of components, applications, and distribution technologies. The basic regulatory regime governing broadband services remains unsettled.[17] In this context, there is no single set of laws or regulations that

governs broadband security or the service and product providers at each level of the food chain. However, this lack of clarity does not mean that broadband security exists in a legal vacuum. Existing industry-specific privacy and security laws, FTC enforcement activities, and common-law precedent in the area of negligence are converging to create general standards for online and database security which must inform the discussion of the security obligations that apply to broadband product and service providers.

Because security is a moving target, packaging security obligations in a neat, legal box is impossible. The emergence of new technologies begets the emergence of new ways to compromise them. The FTC has recognized that "security is more a process than a state"[18] and that standards may differ by industry and by service provided. Consistent with that approach, many of the laws and enforcement actions addressing security require the creation of processes to handle the issue, rather than the implementation of specific solutions.

A. Industry-Specific Legal Security Laws

The most detailed security laws implemented to date at the federal level are embodied by the Gramm-Leach-Bliley Act ("GLB"),[19] which imposes requirements upon financial institutions to implement measures to maintain the security and integrity of consumer information,[20] and the Health Insurance Portability and Accountability Act ("HIPAA"), which governs the protection of individually identifiable health care information.[21] Both laws require the agencies responsible for implementing and enforcing regulations thereunder to include security standards applicable to covered businesses.[22] GLB authorized the FTC and other agencies[23] to "establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information,"[24] with the objectives of "(1) Ensur[ing] the security and confidentiality of customer records and information; (2) protect[ing] against any anticipated threats or hazards to the security or integrity of such records; and (3) protect[ing] against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[25] The FTC responded to this mandate by developing standards for security processes, rather than requiring the implementation of specific technologies or measures. The Final Safeguards Rule requires covered entities to do the following:

a. Develop, implement, and maintain a comprehensive, written security program that contains administrative, technical, and physical safeguards appropriate to such entity's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it maintains.[26]

b. Designate an employee to coordinate the information security program.

c. Identify reasonably foreseeable risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks.

d. Develop an employee training and management program.

e. Evaluate for flaws information systems, including network and software design, information processing, storage, transmission, and disposal.

f. Test and monitor security program's effectiveness.

g. Ensure that third-party providers are capable of maintaining appropriate safeguards for customer information and are contractually obligated to do the same.

h. Evaluate and adjust the information security program to address revealed vulnerabilities or new threats.[27]

The HIPAA Security Regulations, which were issued in February 2003, took a similar approach.[28] The HIPAA Security Rule mandates more process than substance in order to enable covered entities to determine the appropriate security measures to implement after considering the entities' size, complexity, and technical infrastructure, as well as the cost of the security measures and the likelihood and severity of the identified risks.[29]

B. Federal Trade Commission Trends

The FTC has taken a similar, process-oriented approach to defining responsible security practices. It did so in the context of consent decrees arising out of investigations of Eli Lilly and Company ("Eli Lilly"), Microsoft Corp ("Microsoft"), and Guess?, Inc. ("Guess") for alleged misrepresentations as to the level of security each respondent's website or products provided to consumers.[30] The FTC required each respondent to "establish and maintain an information security program" that included, *inter alia*, the following elements:

1. The designation of appropriate personnel to coordinate, oversee, and be accountable for the program;[31]

2. The identification of reasonably foreseeable internal and ex ternal risks to security, including those posed by lack of train ing, and addressing such risks by

    a. creating an appropriate employee training and management program;

    b. evaluating information systems for the processing, storage, transmission, and disposal of information; and

    c. implementing methods to prevent and respond to attacks, intrusions, or other systems failures.

3. The design and implementation of reasonable safeguards to control the risks identified and regular testing and monitor ing of the effectiveness of the safeguards' key controls, sys tems, and procedures.

4. The evaluation and adjustment of the information security program in light of the results of the testing and monitor ing, any changes to respondent's operations or business ar rangements, or any other circumstances that respondent knows or has reason to know may have a material impact on its information security program.

5. The institution of regular third-party audits to ensure the program's adequacy.[32]

The FTC's actions in the Guess, Microsoft, and Eli Lilly cases echo recommendations from the FTC Advisory Committee on Online Access and Security. In May 2000, the Committee noted that computer security was an evolving process and that "anyone who sets detailed computer security standards . . . must be prepared to revisit and revise those standards on a constant basis."[33] To that end, the Committee recommended that companies view security programs as "a continuous life cycle designed to meet the needs of the particular organization or industry. The life cycle should begin with an assessment of risk [and continue with] the establishment and implementation of a security architecture and management of policies and procedures based on the identified risk; training programs, regular audits and continuous monitoring; and periodic reassessment of risk."[34]

C. State Developments

While most states have not addressed the issue of security in the same level of detail as the federal agencies tasked with implementing guidelines under statutory mandate, there are a few developments worth noting. In 2003, California enacted a law requiring the prompt

disclosure of any breach of a network security system that results in the acquisition of unencrypted personal information by an unauthorized person.[35] The law does not mandate specific processes for maintaining information security, but the fact that it applies to breaches of unencrypted personal information and not to disclosures of encrypted information creates a strong incentive for companies doing business in California to employ encryption as part of their security practices.[36]

The law's application to the actual security processes employed by software and service providers is being tested right now in a class-action lawsuit against Microsoft. The plaintiff alleges that she sustained damage as a result of security flaws in Microsoft's Windows operating system. She claims that Microsoft ran afoul of the California statute by failing "to provide adequate and effective notice of security risks created in part due to Microsoft application integration and complexity."[37] The litigation is in its initial stages and it remains to be seen whether it will survive. However, the case raises the question whether service providers, who are aware of security risks inherent in their service or technology, have a duty to provide clear and effective notice to their customers of those risks, and, to the extent possible, provide information on ways to mitigate them.

Finally, a 2002 settlement between three state attorneys general and Ziff-Davis went slightly further than the FTC in mandating specific steps that the online publisher had to take in the wake of the accidental disclosure of customer information.[38] Specifically, Ziff-Davis was required to:

- encrypt sensitive data during transmission from customers;
- control file access through user authentication and application controls;
- monitor and control server activity;
- review applications prior to implementation;
- implement risk identification and response protocols;
- establish management oversight and employee training programs; and
- update its practices to keep pace with evolving industry standards for the privacy, security, and integrity of consumer data.

D. Implied Duty of Care

In the absence of specific statutes governing broadband security, the question becomes whether there is some sort of common law duty to maintain secure services – an implied duty of care. Under this theory, a broadband provider that fails to take "reasonable steps" to cure a security flaw could be deemed negligent.[39] It is difficult to see the law requiring providers to sell "bulletproof" services. Even the plaintiffs in the Microsoft security litigation have not claimed that Microsoft had a duty to sell flawless products. They focus on the deficiencies in Microsoft's notification and remediation processes. Accordingly, the law may evolve in a direction that imposes liability on providers that (a) do not adequately assess the flaws in their systems or services; (b) become aware of security vulnerabilities but choose not to take steps to cure them; or (c) become aware of security vulnerabilities and fail to inform customers about the problems and potential protective measures.[40]

GLB, HIPAA, and the FTC consent decrees also incorporate the concept of "reasonableness" in identifying foreseeable risks and taking appropriate precautions to address them. By its nature, reasonableness will be assessed on a case-by-case basis in light of the specific details of the breach and the business at issue.[41] However, there are indicia of reasonableness that courts or regulatory agencies likely will use as benchmarks. Industry standards and available security tools will become important points of reference when assessing whether a provider has taken reasonable steps to identify and address security risks.

In the broadband world, security standards are being incorporated into new technologies as they develop. For instance, the DOCSIS®[42] specification, applicable to high speed Internet access over cable television infrastructure, incorporates components relating to encryption of transmitted packets as well as authentication of devices that send and receive data over the network. Similarly, the Packetcable™ specification, which sets technical standards for VOIP equipment, contains security features designed to reduce the risk of packet sniffing, eavesdropping, and unauthorized use of service. Hardware vendors who sell equipment to cable operators and subscribers build their devices in compliance with these standards. However, with both DOCSIS and Packetcable, it is up to the cable operator to decide whether to turn on the available security tools.[43]

Further, the government itself is creating *de facto* standards through a number of agencies. The National Institute of Standards and Technology is tasked with developing technical, physical, administrative, and management standards and guidelines to maintain the security and privacy of sensitive information in federal computer systems.[44] These standards for the federal government's systems are incorporated regularly into standards developed by private industry and engineering groups. They set a baseline

definition of reasonable, available security standards and processes that private businesses ignore at their peril. The Department of Homeland Security ("DHS") also is beginning to set standards for the government that likely will apply to private industry. In its "National Strategy to Secure Cyberspace," DHS invokes private industry to participate in its efforts to reduce vulnerabilities in the nation's infrastructure.[45]

III. How Can Broadband Providers Minimize Risk?

In the face of evolving legal standards, broadband providers can minimize the potential for liability by taking a three-pronged approach that includes the following elements: (1) Process – the establishment of a security program that follows the general guidelines set forth in GLB, HIPAA, and the FTC and state consent decrees and is informed by applicable industry security standards; (2) Notice – the provision to customers of information about known security risks as well as information about steps customers can take to protect themselves; and (3) Contractual – ensuring the existing customer agreements disclaim implied warranties and liability for security failures to the extent permissible by law.

A. Process

Implementing a program to identify and address security flaws in broadband services benefits broadband providers in two ways. First, it minimizes the risk of a security breach. Second, companies that implement and maintain effective security programs are more likely to be deemed to have taken reasonable steps to maintain security in the event of a breach – which may influence liability and reduce the measure of damages assessed in the event of a breach.

As discussed above, industry-specific guidelines as well as those issued by the FTC and states in the context of consent decrees set forth the elements of a good security program. While these guidelines generally address a company's internal security measures (*i.e.*, those intended to protect customer information maintained by the company), they include measures applicable to broadband product and service providers.

(1) Define the goal of the security program and identify the systems and other components that are being protected. The program should be designed to provide administrative, technical, and physical safeguards to information held by the provider. The provider also must identify the elements of its network that must be protected. Defining the universe that must be protected is a prerequisite to identifying and implementing appropriate security measures.

(2) Designate an employee or group of employees to coordinate and be accountable for the information security program. The employee does not necessarily have to be dedicated to security full time. However, the FTC consent decrees, GLB, and HIPAA each require that an individual or set of individuals be held accountable for the implementation and continued maintenance of the security program.[46] Since most broadband providers already have resources in their network operations centers or their teams dedicated to controlling network abuse, it may be logical to house the security function within one of those areas. But there should be oversight at an executive level to ensure that the program receives sufficient resources to be effective.

(3) Assess foreseeable risks. Broadband providers must assess the vulnerabilities in their networks, their interfaces to customer equipment, and in their hardware, software, and transmission technology. In performing this analysis, it is important to understand the likelihood of specific threats, the potential harm that could result from specific attacks, and the sufficiency of any safeguards in place to control those risks.[47]

(4) Design and Implement reasonable safeguards against known risks. This is where industry standards become critical. To the extent industry standards or specifications include security tools, such as encryption and authentication measures, it is important for a provider to use those available safeguards. If a company chooses not to do so, that decision should be made only after a rigorous assessment of the risks of ignoring the safeguards and the rationale for doing so. For instance, if using a certain type of encryption adversely affects the quality of a service, deciding not to activate it may be a sensible decision. However, it is critical to go through a risk/benefit analysis to ensure that these decisions are not made lightly. A broadband provider also should regularly test or otherwise monitor the effectiveness of the safeguards it implements.[48]

Broadband providers have at their disposal a number of measures they can implement as part of their program, including the following:

- DOCSIS and Packetcable compliant equipment includes encryption and authentication components that, when activated, make the broadband network and services that pass over the network more secure.

- Dynamic IP address assignment by operators enhances security by making broadband subscribers less static targets for attackers.

- Wireless Equivalent Privacy provides additional security to wireless home networks using 802.11(b)-compatible devices. This solution does not provide complete protection, but in the absence of more robust solutions, it is better than nothing.

- Port blocking by providers can limit the use of certain ports through which malicious or insecure applications or communications pass.

- Recommending that customers change default passwords immediately upon activating their service or equipment can reduce incidents of hacking.

(5) Implement Employee Training and Education. The success of any security program rests largely on educating the employee pool to understand the importance of security, spot risks when they arise, and respond to problems by contacting the appropriate people in the organization. Therefore, it is important to implement a program that reaches all levels of the organization that in any way touch customers or affect operations relating to security.

(6) Ensure that ancillary product or service providers are bound to comply with the security practices and guidelines of the broadband provider. Broadband service includes multiple components, including networks, data transport, hardware, software, content, and applications. A broadband provider should take available steps to ensure that elements provided by third parties are aligned with its own security requirements. This can be accomplished contractually, as well as by ensuring that equipment attached to the network meets industry standard security requirements. Because there are so many elements to broadband service and because subscribers have significant control over what applications and software they use, broadband providers cannot contract against every possible risk. But to the extent they do have business relationships with ancillary providers, they should manage them to reduce risk as much as possible.

(7) Evaluate and adjust the security problem to ensure that it is effective and to meet new threats. As discussed above, security is a process. Accordingly, any effective security program must constantly evaluate its components to determine whether they need to be improved. Similarly, a broadband provider must be aware of new threats as they arise and take measures to respond to them nimbly.

B. Notice

As providers of services, applications, and equipment to consumers and businesses, broadband companies at all levels of the distribution chain should evaluate what type of information to provide to customers regarding security vulnerabilities as well as information about the steps customers can take to protect themselves. Educating

customers about existing risks and available solutions will help reduce the success rate of malicious attacks. In addition, companies that provide this information to customers give themselves ammunition to use against claims of deceptive or unfair practices.[49]

(1) Accurately represent security risks and solutions to consumers. An educated consumer is a less vulnerable consumer. For that reason, and for purposes of setting reasonable expectations of the benefits and risks associated with broadband technologies, it is important to provide consumers with clear and accurate information about security. Consumers who are armed with this information can determine for themselves what level of risk they are willing to live with. Broadband companies have a number of vehicles through which they can provide this information to existing or potential customers. They can dedicate portions of their websites to security issues, publish Frequently Asked Questions ("FAQs") relating to security, and recommend specific steps customers should take in order to protect their home networks and equipment.[50]

(2) Stay aware of new security threats and create notification process in the event of a known breach. It is important for broadband providers to stay aware of new security threats and communicate them to customers as they arise. This is the case even when a problem arises from a source beyond the control of the broadband provider – such as a software glitch, a vulnerability in an industry standard security protocol, or a problem with third-party equipment. Early notification can help avoid harm to the provider's network as well as to customer equipment.

To the extent new threats relate specifically to broadband, it is critical to disseminate information to customers so that they can protect against those risks. In order to do so effectively, broadband providers should establish processes by which information about threats that are identified can be evaluated internally and communicated externally in a clear, understandable manner. Creating a cross-functional "SWAT Team" that includes technical, legal, and public relations expertise can help an organization respond quickly and effectively to new problems.

(3) Offer security solutions to customers when possible. It is not strictly necessary to provide security solutions to customers – particularly when solutions like firewall or anti-virus software are available commercially. However, incorporating security solutions into a product or service can ease the burden on consumers to evaluate technical solutions on their own. Security solutions can be home-grown, bundled with a product or service, or offered as a premium or add-on.

(4) Don't misrepresent the level of security provided. Companies that have run afoul of the state and federal consumer protection agencies due to security problems generally have done so as a result of express or implied misrepresentation of the level of security they offer.[51] Broadband companies should avoid puffing the security features they offer or claiming superiority over competitors in the security arena. Microsoft's statements regarding the security features of its Passport application are precisely what drew FTC scrutiny. To this end, counsel for broadband providers should vet marketing materials closely for claims of imperviousness. In addition, counsel should ensure that customer service and sales personnel are trained to understand the dangers of minimizing or dismissing security concerns voiced by existing or potential customers. Finally, where products or services are sold through third-party sales channels, such as retail outlets, sales personnel need to be trained on the appropriate way to describe security.

C. Contractual Protections

The relationship between broadband providers and customers ultimately is defined by contract. Providers should use the contract as another tool through which to define the scope of their responsibility and limit their liability for ensuring customer security. To this end, it is important to include in customer contracts limitations and disclaimers of liability for security breaches, damage to equipment or software, loss of data, and other consequential damages. This language is standard; however, broadband providers should include security-specific language to avoid any ambiguity as to the scope of their legal responsibility. Similarly, providers of broadband services should include language permitting them to manage their networks and impose security solutions that they deem appropriate (even if they have the side effect of degrading service or blocking the use of certain applications). Without this flexibility, providers could find themselves in the unenviable position of withholding a security solution for fear of changing features of the service they had marketed to customers. Finally, it is critical that providers establish procedures that require that these contracts are actually signed or clicked through by customers. The most protective language loses its effect if the contract is deemed unenforceable by virtue of a lack of agreement.

Conclusion

The opportunities created by broadband engender risk. Broadband is no exception to the observation that legal standards rarely keep pace with technological developments. In this uncertain environment, broadband service and product providers have no

fixed formula by which they can protect their customers from security breaches and insulate themselves from liability arising out of those breaches. However, by employing a flexible approach to security that generally incorporates the measures discussed above, broadband providers may be able to mitigate the security risks that they and their customers face.

P

(Endnotes)

[1] Leslie F. Spasser is a partner of the Norfolk, Virginia-based law firm, Willcox & Savage P.C. She counsels clients on privacy, technology and communications law issues. Prior to joining Willcox, Ms. Spasser served as Senior Counsel to Cox Communications, Inc., where she worked closely with the company 's product development and new services teams.

[2] In keeping with his creative language choices and inappropriate use of unsolicited e-mail as a means of raising security awareness among others, Mr. Nasty concluded his missive with a link to a pornographic web site.

[3] 15 U.S.C. §§ 6801(b), 6805(b)(2); 42 U.S.C. §§ 1302(d)-2 & 1320(d)4.

[4] *See, In re: Matter of Guess?, Inc. & Guess.com, Inc.*, File No. 0223260 (Aug. 5, 2003), available at http://www.ftc.gov/opa/2003/08/fyi0348.htm ("Guess Consent Decree"); *In re: Microsoft Corp.*, File No. 0123240, Agreement Containing Consent Order (Aug. 7, 2002), available at http://www.ftc.gov/os/2002/08/microsoftagree.pdf ("Microsoft Consent Decree"); and *In re: Eli Lilly & Co.*, File No. 0123214, Decision and Order (May 8, 2002), available at http://www.ftc.gov/os/2002/05/elililly do.htm ("Eli Lilly Consent Decree").

[5] *See Marcy Levitas Hamilton v. Microsoft Corp.*, which can be found at www.computerbytesman.com/security_hamilton_v_microsoft_complaint.htm.

[7] Standard cable broadband offerings provide speeds of 256 kilobits per second upstream (to the Internet) and 1.5 to 3 Megabits per second downstream (to the PC), although many operators offer higher speed tiers for businesses and high-volume users.
DSL offerings differ from market to market, but provide speeds from 129 kbps upstream/256 kbps downstream to 256 kbps upstream/1.5 Mbps downstream.

[8] "Home Network Security," CERT Coordination Center, Carnegie Mellon University, Section 11(D) found at http://www.cert.org/tech_tipshome_networks.html ("CERT Home Networking Paper").

[9] Trojan horse programs allow intruders to trick unsuspecting computer users to install "backdoor" programs. These can allow intruders access to a consumer 's computers without the consumer's knowledge and enable the intruder to change system configurations, infect the computer with a virus, and otherwise remotely control the computer. *See* CERT Home Networking Paper at 8.

[10] When broadband providers assign static (unchanging) IP addresses to customers, this vulnerability is especially acute. Dynamic IP addressing, where IP addresses of specific customers change periodically, can help mitigate this risk. *See* CERT Home Networking Paper at 6.

[11] See Stump, Matt, "Rivals at the Gates Eye Share of Home," *Multichannel News*, Jan. 12, 2004, p.4 (discussing the announcements by Microsoft executives during the Consumer Electronics Show of plans to use software to link devices within the networked home and enable consumers to move it from the TV to the PC to other devices).

[12] *See, e.g.*, Messmer, Ellen, "Wireless LAN Security Worries on Horizon," *Computerworld*, Jan. 13, 2004, found at http://www.computerworld.com/printthis/2004/0,484,89026,00.html (discussing the flaws in the Wired Equivalent Privacy standard and the difficulty and cost inherent in upgrading to the more secure 802.11i protocol); Crockett, Roger O., "For Now, Wi-Fi Is A Hacker's Delight," *BusinessWeek Online*, Jan. 19, 2004, found at http://www.businessweek.com:/print/magazine/content/04_03/b3966086_mz063.htm?tc (discussing the phenomenon of "drive by hacking" and the necessity for new security standards to protect corporate wi-fi networks from intruders); Shim, Richard, "Wi-Fi Arrest Highlights Security Dangers," *CNET News.com*, Nov. 28, 2003, found at http://zdnet.com.com/2100-1105_2-5112000.html (detailing the arrest of a man in Canada for allegedly downloading child pornography over a hijacked wi-fi connection).

[13] Kuhn, Richard D. , Tracy, Miles C., Frankel, Sheila E., "Security for Telecommuting and Broadband Communications, Recommendations of National Institute of Standards and Technology," U.S. Department of Commerce, Special Publication 800-46, Aug. 2002, p.44 ("NIST Broadband Security Recommendations").

[14] NIST Broadband Security Recommendations at 44-45.

[15] The British government recently raised an alarm about security flaws in products that enable VOIP, which had the potential effect of allowing attackers to take control of VOIP systems. *See* "Flaws threaten VoIP Networks," *CNET News.com*, Jan. 13, 2004, found at http://news.com.com/2100-1002-5140284.html; "Vulnerability Note VU#749342," CERT Coordination Center, Carnegie Mellon University, found at http://www.kb.cert.org/vuls/id/749342.

[16] Final HIPAA Security Regulations, 45 CFR Parts 160, 162, and 164.

[17] The FCC classified cable modem service as an "Interstate Information Service." However, it currently is evaluating the extent to which it should regulate cable broadband service and whether there are "legal and policy reasons why" other wireline broadband services, such as DSL, should be treated differently. *See In re: Inquiry Concerning High Speed Access to the Internet Over Cable and Other Facilities*, CS Docket No. 02-52 (Mar. 15, 2002) at 72.

[18] Final Report of the FTC Advisory Committee on Online Access and Security, May 15, 2000, p.26, found at http://www.ftc.gov/acoas/papers/finalreport.htm. (hereinafter, "FTC Security Report").

[19] 15 U.S.C. §§6801(b), 6805(b)(2).

[20] *Id.*

[21] 42 U.S.C. §§1320d-2 & 1320d-4.

[22] Standards for Safeguarding Customer Information; Final Rule, 16 CFR Part 314.

[23] Other agencies also were authorized to establish safeguards standards, including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, the Secretary of the Treasury and the Securities and Exchange Commission.16 CFR Part 314.

[25] 15 U.S.C. § 6801(b)(1)-(3).

[26] 16 CFR § 314.3

[27] 16 CFR § 314.3-4.

[28] The HIPAA Security Rule requires covered entities to (1) ensure the confidentiality, integrity, and availability of electronic health information; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information, and 3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required. 45 CFR Parts 160, 162, and 164.

[29] *See* Guess Consent Decree, Microsoft Consent Decree, Eli Lilly Consent Decree.

[30] *See supra* note 29.

[32] *Id.*

[33] FTC Security Report at 26.

[34] *Id.*

[35] Cal. Civ. Code § 1798.82.

[36] The FTC also has emphasized the importance of notifying individuals as soon as possible if they are affected by an information security breach, although it has not implemented regulations to that effect. *See* Prepared Statement of the Federal Trade Commission on Identity Theft: Prevention and Victim Assistance, Before the Subcommittee on Oversight and Investigations of the House Committee on Energy and Commerce, Langhorne, PA, Dec. 15, 2003.

[37] *See Hamilton v. Microsoft Complaint.*

[40] *See* Smedinghoff, Thomas J., "The Developing Legal Standard for Cybersecurity," 4 Sedona Conf. J. 109, 113 (Fall 2003).

[41] 45 CFR § 164.306(b).

[42] Data Over Cable Service Interface Specification, developed by Cable Laboratories, Inc. to facilitate the interoperability of cable modems and associated equipment.

[43] Similar standards have been developed in the wireless space, where different levels of encryption of data can be employed by equipment makers and consumers. However, existing security standards, such as Wireless Equivalency Protocol ("WEP"), have known vulnerabilities that permit attackers to access wireless networks with relative ease. *See* NIST Broadband Security Recommendations at 44. Wireless networks also are subject to denial of service attacks. *Id.*

[44] *Id.* at iii.

[45] "National Strategy to Secure Cyberspace, Feb. 14, 2003, found at http://www.whitehouse.gov/pcipb.

[46] *See* Microsoft Consent Decree, Guess Consent Decree, Eli Lilly Consent Decree, 16 CFR § 314.4(a)).

[48] GLB, 16 CFR § 314.4(c), *See also* Guess Consent Decree.

[49] *See* Microsoft Consent Decree; Eli Lilly Consent Decree; Guess Consent Decree.

[50] For instance, providing information about the importance of firewalls for computers attached to broadband connections, as well as for home networks, can help customers avoid attacks. Similarly, providing educational materials about antivirus software and other protective technologies also can circumvent attacks.

[51] *See* Microsoft Consent Decree, Eli Lilly Consent Decree, Guess Consent Decree.

Consumer Protection Committee

John Villafranco
Vice-Chair
Collier Shannon Scott PLLC
Washington, DC
jvillafranco@colliershannon.com

Julie Brill
Vice-Chair
Office of the Attorney General
of the State of Vermont
Montpelier, VT
jbrill@atg.state.vt.us

Lesley A. Fair
Vice-Chair
Federal Trade Commission
Washington, DC
lfair@ftc.gov

August Horvath
Vice-Chair
Weil, Gotshal & Manges LLP
New York, NY
august.horvath@weil.com

Computer and Internet Committee

David H. Evans
Co-Chair
Arent Fox Kintner Plotkin & Kahn, PLLC
Washington, DC
evans.david@arentfox.com

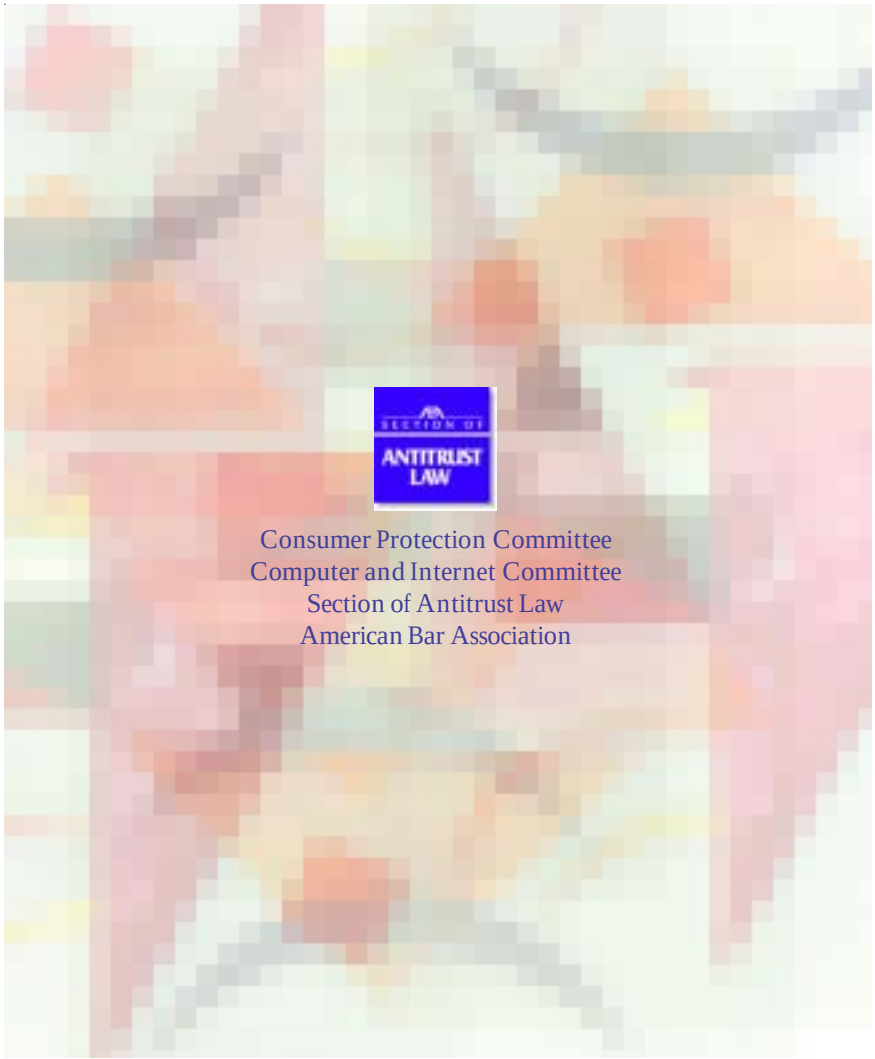
Leslie C. Overton
Co-Chair
Department of Justice
Washington, DC
loverton@

Mark C. Del Bianco
Vice-Chair
Kensington,MD
mark@markdelbianco.com

Patrick Kelleher
Vice-Chair
Gardner Carton & Douglas
Chicago, IL
pkelleher@gcd.com

Gail Levine
Vice-Chair
Federal Trade Commission
Washington, DC
glevine@ftc.gov

Paul Saint-Antoine
Vice-Chair
Drinker, Biddle & Reath LLP
Philadelphia, PA
paul.saint-antoine@dbr.com



Consumer Protection Committee
Computer and Internet Committee
Section of Antitrust Law
American Bar Association