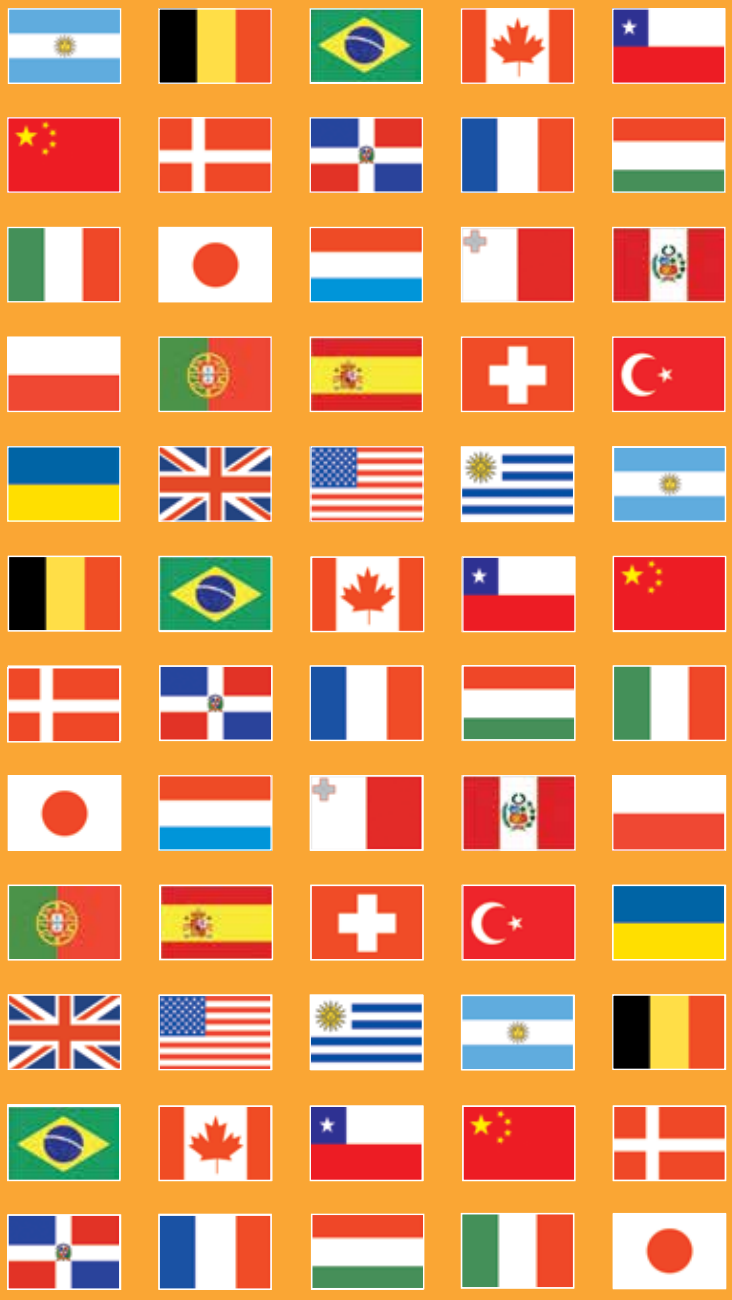
GETTING THE DEAL THROUGH

e-Commerce 2015

in 24 jurisdictions worldwide

2015

Contributing editor: Robert Bond



Published by
Getting the Deal Through
in association with:

Aird & Berlis LLP

Angeles & Lugo Lovatón

B+B Law Firm

Bird & Bird Advokatpartnerselskab

Bogsch & Partners Law Firm

Bühlmann Attorneys at Law

Caiado Guerreiro & Associados

Ferrere

García Magliona y Cía Abogados

Iriarte & Asociados

Karniol Małecki i Wspólnicy spk

Marx Van Ranst Vermeersch & Partners

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

Monereo Meyer Marinel-lo Abogados

Nobles

Orsingher Ortu – Avvocati Associati

Parness Law Firm, PLLC

Sarrut Avocats

Speechly Bircham LLP

Stibbe

Vitale, Manoff & Feilbogen

WH Partners

Yuasa and Hara

Zhong Lun Law Firm

e-Commerce 2015

Contributing editor: Robert Bond Speechly Bircham LLP

Getting the Deal Through is delighted to publish the eleventh edition of *e-Commerce,* a volume in our series of annual reports, which provide international analysis in key areas of law and policy for corporate counsel, cross-border legal practitioners and business people.

Following the format adopted throughout the series, the same key questions are answered by leading practitioners in each of the 24 jurisdictions featured. New jurisdictions this year include Belgium, Brazil, Canada, Denmark, Hungary and Portugal. This year the volume features chapters on Monitoring in the Workplace and The Growth of Outsourced Solutions.

Every effort has been made to ensure that matters of concern to readers are covered. However, specific legal advice should always be sought from experienced local advisers. ***Getting the Deal Through*** publications are updated annually in print. Please ensure you are referring to the latest print edition or to the online version at www.gettingthedealthrough.com.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We would also like to extend special thanks to contributing editor Robert Bond of Speechly Bircham LLP for his continued assistance with this volume.

Getting the Deal Through
London
July 2014

Monitoring in the workplace: a French case study 3
Raphaël Dana
Sarrut Avocats

The growth of outsourced solutions: data protection – the practical considerations 6
Janine Regan
Speechly Bircham LLP

Argentina 8
Héctor Ariel Manoff, Nicolás Matías Czejer and Vanesa Balda
Vitale, Manoff & Feilbogen

Belgium 14
Jan Ravelingien and Carl Kestens
Marx Van Ranst Vermeersch & Partners

Brazil 20
Fabio Ferreira Kujawski
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

Canada 27
Donald B Johnston
Aird & Berlis LLP

Chile 33
Claudio Magliona
García Magliona y Cía Abogados

China 38
Jihong Chen
Zhong Lun Law Firm

Denmark 43
Nis Peter Dall
Bird & Bird Advokatpartnerselskab

Dominican Republic 49
Jaime R Ángeles
Angeles & Lugo Lovatón

France 55
Raphaël Dana and Tressy Ekoukou
Sarrut Avocats

Hungary 61
Ádám Liber and Tamás Gödölle
Bogsch & Partners Law Firm

Italy 69
Marco Consonni
Orsingher Ortu – Avvocati Associati

Japan 78
Kozo Yabe and Takeshi Kanda
Yuasa and Hara

Luxembourg 84
Dirk Leermakers and Nicolas van Heule
Stibbe

Malta 90
Olga Finkel
WH Partners

Peru 97
Erick Iriarte Ahón and Fátima Toche Vega
Iriarte & Asociados

Poland 102
Robert Małecki
Karniol Małecki i Wspólnicy spk

Portugal 108
Ricardo Rodrigues Lopes and Vanessa Vicente Bexiga
Caiado Guerreiro & Associados

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Rachel Nurse
subscriptions@gettingthedealthrough.com

Business development managers
George Ingledew
george.ingledew@lbresearch.com

Alan Lee
alan.lee@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2004
11th edition
ISSN 1473-0065

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Spain 114

Belén Arribas Sánchez
Monereo Meyer Marinel-lo Abogados

Switzerland 119

Lukas Bühlmann
Bühlmann Attorneys at Law

Turkey 126

Sıdıka Baysal Hatipoğlu, Gökhan Uğur Bağcı and Benan İlhanlı
B+B Law Firm

Ukraine 131

Volodymyr Yakubovskyy and Alexander Weigelt
Nobles

United Kingdom 136

Robert Bond
Speechly Bircham LLP

United States 147

Hillel I Parness
Parness Law Firm, PLLC

Uruguay 157

Alejandro Alterwain and Martín Cerruti
Ferrere

United States

Hillel I Parness*

Parness Law Firm, PLLC

General

1 How can the government's attitude and approach to internet issues best be described?

The US federal government has taken an aggressive approach towards the internet in a number of different areas, including intellectual property, speech, inter-governmental regulation and children's privacy. The US administration has implemented a number of its internet priorities, including the appointment of a 'cyber czar' with a mandate to coordinate US defences against hacker attacks and the use of economic stimulus funds to expand broadband web access to rural areas. In addition, the US administration has been advancing controversial 'net neutrality' rules mandating that high-speed internet providers disclose information about their services, refrain from blocking most content and transmit lawful network traffic without discriminating based on the identity of the content provider. In June 2014, a set of proposed rules for net neutrality were approved by the US Federal Communications Commission (FCC) for further proceedings. Although the new rules would authorise internet service providers (ISPs) to charge some websites for faster service, they would also permit internet users to have open access to online information without an additional cost. Because internet-related legislation is often reactive to particular situations or concerns, it has been observed that the resulting coverage is in some respects uneven. Others have raised the concern that the pace of advancing technology makes legislation difficult, and can result in unintended consequences as legislation strains to keep up. The United States and approximately 20 other nations declined to sign amendments to the International Telecommunications Regulations (ITRs) concerning international regulation of the internet. US Ambassador Terry Kramer explained that the United States does not support the treaty because 'internet policy should not be determined by member states but by citizens, communities and broader society, and such consultation from the private sector and civil society is paramount.' Commissioner Robert McDowell of the US FCC stated that 'nations supporting the treaty "chose to discard long-standing international consensus to keep the internet insulated from intergovernmental regulation."' Another round of negotiations on the ITRs will take place some time this year.

Legislation

2 What legislation governs business on the internet?

Some of the more prominent US laws that touch upon internet business issues are set forth briefly here.

- Federal Trade Commission Act of 1914, 15 USC, sections 41–58: prohibits unfair or deceptive advertising in any medium, including internet advertising.
- 'Good Samaritan' provision of the Communications Decency Act of 1996 (CDA), 47 USC, section 230(c)(1): shields the 'provider(s) or user(s) of an interactive computer service' from being 'treated as the publisher or speaker of any information provided by another information content provider'. Originally enacted to immunise service providers from secondary liability for defamation by users, this provision has been used to exempt a wide range of internet-based entities from various types of speech-based violations.
- Online Copyright Infringement Liability Limitation Act of the Digital Millennium Copyright Act of 1998 (DMCA), 17 USC, section 512: establishes a complex group of safe harbours for internet-based entities from secondary copyright infringement liability if they react expeditiously to notices of primary infringement and meet other procedural requirements.
- Anti-cybersquatting Consumer Protection Act of 1999 (ACPA), 15 USC, sections 1114(2)(D), 1125(d): sets out the standards under which federal lawsuits can be brought in response to the abusive registration of domain names.
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), 15 USC, sections 7701–13, 18 USC, section 1037: imposes limitations and penalties on the transmission of unsolicited commercial e-mail via the internet.
- US Gramm-Leach-Bliley Act of 1999 (GLB), 15 USC, sections 6801–10: requires financial service providers to safeguard customer information, advise customers of the nature of the information which they collect, advise customers with whom they share their information and allow customers to opt out of any sharing of their information.
- Health Insurance Portability and Accountability Act, 45 CFR, section 164.312: requires establishment of national standards for electronic health-care transactions and national identifiers for providers, health insurance plans and employers.
- Children's Online Privacy Protection Act of 1998 (COPPA), 15 USC, section 6501 et seq: requires any commercial website or online service that is targeted to children under the age of 13 to obtain parental consent before collecting personal information. On 1 July 2013, revisions to COPPA imposed restrictions on the ability of third-party affiliates of websites and mobile applications directed at children to collect user data. As the burden for compliance with these new regulations falls upon the service providers, there is substantial discussion over the policy and technology changes that companies will need to make to ensure ongoing compliance.
- Electronic Communications Privacy Act, 18 USC, section 2510: addresses interception and disclosure of wire, oral or electronic communications, extending pre-existing coverage to new forms of communication. The scope of protection offered by this act is disputed. Compare *Brahmana v Lembo*, 2009 US Dist Lexis 42800 (ND Cal 20 May 2009) (holding that keystrokes captured by a keylogging device may be protected electronic communications) with *United States v Ropp*, 347 F Supp 2d 831 (CD Cal 2004) (opposite result).
- Computer Fraud and Abuse Act 1986, 18 USC, section 1030, et seq: addresses improper access or 'hacking' of computer

systems. 2001 amendments under the USA Patriot Act increased its applicability and range of penalties.
- Unlawful Internet Gambling Enforcement Act (UIGEA) of 2006, 31 USCS, sections 5361–67: regulates online gambling by prohibiting any person in the business of betting or wagering from knowingly accepting payment from a person who participates in unlawful internet gambling.
- Keeping the Internet Devoid of Sexual Predators Act of 2008: requires social networking websites to search their users for matches to the National Sex Offender Registry.
- Broadband Data Improvement Act of 2008: seeks to improve the quality of federal broadband data collection and encourages state initiatives that promote broadband deployment.
- The Prioritizing Resources and Organization for Intellectual Property Act of 2008, 15 USCS, section 8101: expands the scope of liability and remedies resulting from online piracy and counterfeiting and creates an Intellectual Property Enforcement Coordinator within the executive branch.
- Article 2 of the Uniform Commercial Code (UCC) has applicability to the buying and selling of goods on the internet.
- Federal Trade Commission Net Neutrality Rules, 25 FCC Rcd 17905: mandates that high-speed internet providers disclose information about their services, refrain from blocking most content and transmit lawful network traffic without discriminating.

Regulatory bodies

3 Which regulatory bodies are responsible for the regulation of e-commerce and internet access tariffs and charges?

The following entities are primarily responsible for the regulation of e-commerce and internet access:
- the FCC: regulates interstate and international communications by radio, television, wire, satellite and cable, including telecommunications across the internet;
- the Federal Trade Commission (FTC): enforces both consumer protection and antitrust laws and protects consumers against 'unfair' or deceptive acts or practices in commerce;
- the Federal Financial Institutions Examination Council: sets uniform principles, standards and report forms for the federal examination of financial institutions, and promotes uniformity in the supervision of financial institutions; and
- the Advisory Commission on Electronic Commerce: studies federal, state, local and international taxation and tariffs on transactions using the internet and internet access.

Jurisdiction

4 What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions (or disputes) in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Since 1997, a body of case law has been formed that guides courts in determining whether and under what circumstances internet activity can create personal jurisdiction over parties. Although no bright-line test exists, most courts draw a distinction between 'interactive' and 'passive' websites. Thus, many courts will extend jurisdiction over the proprietor of a website that purposefully interacts with residents of a particular jurisdiction. However, maintaining a passive website that does not purposefully interact with the occupants of a particular jurisdiction, is less likely, standing alone, to create jurisdiction over the website owner. For example, in *Best Van Lines Inc v Walker*, 490 F 3d 239 (2d Cir 2007), the Court of Appeals for the Second Circuit found that the proprietor of a not-for-profit internet website located in Iowa did not, merely by posting derogatory comments about a New York moving company, 'transact business' within New York for jurisdictional purposes. By way of contrast, in *Bridgeport Music Inc v Still N The Water Pub*, 327 F 3d 472 (6th Cir 2003), the Court of Appeals for the Sixth Circuit held that the operation of a website can lead to jurisdiction if it is shown that the defendant, through the interactive website, engaged in purposeful interaction with residents of the state, and remanded the case for further findings. See also *Zippo Mfg. Co v Zippo Dot Com Inc*, 952 F Supp 1119 (WD Pa 1997) (holding that the court has personal jurisdiction over defendant since defendant's conducting electronic commerce with the state's residents constituted a purposeful availment of doing business in the state). To determine whether online activities could subject a defendant to personal jurisdiction, some courts still apply the '*Calder* effects test' despite the fact that internet commerce was non-existent at the time of *Calder v Jones*, 465 US.783, 104 S. Ct. 1482, 79 L. Ed. 2d 804 (US. 1984). According to '*Calder* effects test', the defendant must (1) commit an intentional act that is (2) expressly aimed at the forum state that (3) causes harm that the defendant knows is likely to be suffered in the forum state. Courts generally have declined to extend personal jurisdiction solely on the basis of website advertising. Furthermore, the courts have declined to extend personal jurisdiction when the party merely transmits or enables the transmission of information via the internet without selecting or knowingly directing that information to the forum state, see *ALS Scan, Inc v Digital Serv Consultants Inc*, 293 F.3d 707 (4th Cir 2002) (holding that a party that provides bandwidth to another party to enable that second party to electronically transmit information via the internet is not subject to jurisdiction in the forum state where the information transmitted causes an injury).

Courts have also consistently held that a single transaction using an online auction process, such as eBay, is insufficient to create personal jurisdiction over the seller for the purposes of a complaint by a buyer. See, for example, *Boschetto v Hansing*, 539 F 3d 1011 (9th Cir 2008) (granting a motion to dismiss for lack of personal jurisdiction over a eBay seller of a used car, resident in Wisconsin, sued by a buyer, a Californian citizen). Where online auction sellers make a pattern of sales, or communicate a willingness to sell in multiple jurisdictions, however, they may be subject to personal jurisdiction outside of their own state. See, for example, *Dedvukaj v Maloney*, 447 F Supp 2d 813 (ED Mich 2006) (finding defendant online auction seller subject to Michigan jurisdiction because auction listing included a toll-free telephone number and stated that seller would ship anywhere in the United States); and *The AAA v Darba Enters*, 2009 US Dist. Lexis 37564, (N.D. Cal. Apr. 21, 2009) (finding jurisdiction because, among other factors, defendant used pay-per-click advertisements to lure customers, including customers from California). In the opposite situation, where the website is owned by the plaintiff, courts will generally look to forum selection clauses in the website's terms of service, even when the defendant has used the website without authorisation. See, for example, *CoStar Realty Info Inc v Field*, 612 F Supp 2d 660 (D Md 2009) (holding that a Maryland court could exercise personal jurisdiction over out-of-state defendants where these defendants were presented with a forum selection clause during their unauthorised use of plaintiff's online database). Each state's rules for personal justification differ and must be carefully scrutinised in each situation.

Contracting on the internet

5 Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?

It is generally recognised that contracts can be formed and concluded electronically if the terms are clearly conveyed and recorded, and the parties' agreement to the terms of the contract is likewise clearly conveyed and recorded, often (although by no means necessarily) through the use of some form of digital signature. In the well-known case of *Specht v Netscape*, 150 F Supp 2d 585, 595 (SDNY 2001), aff'd, 306 F3d 17 (2nd Cir 2002), the court held that there must

be an 'affirmative action unambiguously expressing assent before they may use the software' for a 'click through' agreement to be enforceable, as contrasted with the 'browse-wrap' licence before the court in that case. However, a click through agreement may be binding when a party did not actually see the agreement, if that party is a sophisticated business entity that should have been aware that a transaction would be accompanied by terms and conditions See *Via Viente Taiwan LP v UPS Inc*, 2009 US Dist Lexis 12408 (ED Tex 17 February 2009) (plaintiff should have been aware of click through agreement in a software program installed by defendant's technician). In 2009, the FTC (see question 3) settled a case against Sears Inc, which was charged with violating section 5 of the FTC Act because it created software programs that, among other things, collected consumers' sensitive personal information. Some consider the FTC's decision to litigate notable in a situation where the consumer at least had the opportunity to review and accept agreements, and a possible signal of heightened requirements for electronic contracts. The drafting of the electronic contract also has an impact on whether or not it is binding. For example, an online contract may be unenforceable if one party reserves the right to modify the terms and conditions at any time, without notice to the other party. See *In re Zappos Inc*, 893 F Supp 2d 1058 (D Nev 2012).

6 Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

The UC Electronic Signatures in Global and National Commerce Act (ESIGN), 15 USC, section 7001, applies to 'any transaction in or affecting interstate or foreign commerce' and validates the use of electronic means to conclude contracts. Under ESIGN, 'a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form', and 'a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation' (ibid, sections 7001(a)(1)-(2)). Certain classes of documents, such as wills, sales under the UCC (see below and question 2), court documents, notices concerning the termination of utilities and insurance, and notices relating to hazardous materials (ibid, sections 7003(a)-(b)) are excluded from ESIGN's scope.

ESIGN does not distinguish between the formation of business-to-consumer and business-to-business contracts, although it does have provisions requiring certain consumer disclosures and consents before entities can implement electronic record keeping (ibid, section 7001(c)(1)).

Forty-seven of the 50 states, the District of Columbia, Puerto Rico and the Virgin Islands have adopted the Uniform Electronic Transaction Act (UETA), 7A ULA 225, which provides a legal framework for the use of electronic signatures and records in government or business transactions. UETA, as expressly defined in articles 3 and 4, only applies to transactions related to business, commercial, and government matters; and to transactions conducted by electronic means. The UETA is permitted to the extent its provisions are not inconsistent with ESIGN. Thus the effect of state law should be considered to the extent applicable to specific transactions or disputes.

The Uniformed Commercial Code (UCC), article 2 refers to the sales of goods and article 2A refers to the lease of goods including computer equipment. The UCC applies to electronic contracts for the sale of goods, however, it does not apply to the online sale of services. Article 2 of the UCC applies to all contracts, both business-to-business and business-to-consumer, for the sale of goods, unless the parties agree to vary the terms of their agreement. Louisiana is the only state that has not adopted article 2, and versions of article 2 vary from state to state.

The Uniform Computer Information Transaction Act (UCITA) is a proposed state contract law developed to regulate transactions in computer information products such as computer software, online databases, software access contracts or e-books. UCITA was designed to clarify issues which were not addressed by existing UCC. At this time, it has been adopted only by Virginia and Maryland.

7 How does the law recognise or define digital or e-signatures?

The law defines 'electronic signature' as 'an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record'. The definition is not limited by or tied to any particular technology. Indeed, ESIGN prohibits enactment of state statutes that do otherwise (ESIGN, 15 USC, section 7002(a)(2)(A)(ii)).

8 Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

ESIGN requires entities to provide consumers with information concerning hardware and software requirements, and also requires notice of changes to hardware or software requirements that create a material risk that consumers will not be able to access their records (ibid, sections 7001(c)(1)(C)-(D)). The UETA, by contrast, adopts a somewhat more relaxed approach toward data retention obligations.

Security

9 What measures must be taken by companies or ISPs to guarantee the security of internet transactions?

There is no single law in the US that provides a comprehensive treatment of internet security issues. However, each of HIPAA, COPPA and GLB statutes (see question 2) has provisions addressing what can and cannot be done with personal or private information, and when disclosures must be made to data subjects about the maintenance and use of their information. Further, a 'sectoral' approach to data protection legislation is adhered by the US. The laws of data protection and privacy depend on, in addition to governmental interference, a combination of legislation, regulation, and self-regulation. Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have data protection laws in place that focus on internet security, generally requiring notification of consumers when security breaches take place. Moreover, five major credit card companies: American Express, Discover, JCB International, MasterCard and Visa formed the Payment Card Industry (PCI) Security Standards Council and in 2004 created and adopted the PCI Data Security Standard (PCI DSS) to establish a uniform, industry-regulated standard to optimise the security of payment card transactions. All organisations or merchants who accept, transmit or store any cardholder data must comply with the regulations set forth by the PCI DSS. The use of encryption to protect sensitive data, such as financial and medical information, is standard e-commerce practice, especially since state consumer protection agencies have pursued claims on information-holding companies. One recent settlement led to a multimillion-dollar payment by a company that failed to notify its customers of unauthorised access to their credit card information. Some states have enacted data protection laws that go beyond simply notifying customers of a security breach. Massachusetts, for example, recently implemented a data security regulation that requires all entities that license, store or maintain personal information about a Massachusetts resident to implement a comprehensive information security programme, even if the business or entity does not have offices in the state.

10 As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

Other than regulation of the exportation of certain types of encryption technology, US laws do not currently address encryption. Encryption received renewed attention following the 9/11 attacks, and legislation was proposed, but not enacted, that would give law enforcement access to private encryption keys, so as to be able to quickly access even encrypted communications. In the noteworthy decision of *In re Boucher*, 2009 US Dist Lexis 13006 (D Vt 2009), the court ordered a US citizen to produce the password to his encrypted hard drive so that the government could access images of child pornography that a governmental agent had already seen during the defendant's initial detention. Similarly, in *US v Hatfield*, 2010 US Dist Lexis 34478 (EDNY 7 April 2010), a defendant was ordered to produce metadata associated with certain documents, in part because his counsel had already acknowledged that the metadata existed. More recently, in *US v Doe* (I*n re Grand Jury Subpoena Duces Tecum*), 670 F 3d 1335 (11th Cir 2012), the Eleventh Circuit Court of Appeals reversed a district court decision holding a defendant in contempt. The appellate court concluded that the defendant could not be compelled to comply with a court order to produce encrypted data where the government had not established that the information it sought was contained in the encrypted data. These cases leave unsettled the question of whether the government can compel production of files where it does not already know if these files are incriminating.

Domain names

11 What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

Domain names are distributed by official domain name registrars, which are accredited by various organisational bodies. Each registrar maintains its own policies and procedures, and is generally subject to de-accreditation by the body that administers the particular top level domain (TLD). Registrars for non-country-specific TLDs (such as '.com', '.net' and '.org') are accredited by the Internet Corporation for Assigned Names and Numbers (ICANN). In 2011, ICANN ended restrictions on becoming a registrar for non-country-specific TLDs and established a new generic top-level domains (gTLD) program. The program allows companies and individuals to apply for domain names ending in words other then territory codes, such as '.flowers' or '.google'. It was developed to increase competition and choice for registry service providers on the internet. Moreover, the program allows gTLDs to end in almost any word in any language, including characters and symbols not in the Latin alphabet. Registrars for country-specific top level domains are typically accredited by the countries to which those TLDs are assigned.

In the case of '.us', the TLD for the US, applicants must certify that they have a 'bona fide presence in the United States', and must satisfy one of three territorial requirements: the registrant must be a US citizen who is a permanent resident or whose primary domicile is the US; the registrant must be a domestic US entity, incorporated within the US or organised under the laws of the US; or the registrant must be a foreign entity with a bona fide presence in the US. The requirement of having a US nexus is ongoing, and the administrator of the '.us' domain states that it monitors registrations for nexus compliance. See www.neustar.us for more information.

On 9 April 2013, ICANN and ICANN-accredited registrars reached a tentative agreement on a new version of the Registrar Accreditation Agreement (RAA), subject to provide increased protection for registrants, enhanced security generally, and increased predictability for all stakeholders. The new RAA was approved by the ICANN board on 27 June 2013 and is obligatory for registrars who deal with new gTLDs, but it is not yet obligatory for .org, .info, or .biz. The new version of the RAA, went into immediate effect for all new and incumbent registrars who wishes to sell domain registrations in new gTLDs, and is in effect with all other registrars as their current agreements expire.

12 Do domain names confer any additional rights (for instance, in relation to trademarks or passing off) beyond the rights that naturally vest in the domain name?

No. Registration of a domain name has no direct bearing on trademark rights. Companies and individuals selecting new names for use in commerce are thus well advised to focus simultaneously upon confirming that the name is free from trademark issues and that it is available for use as a domain name. The registration of a domain name, however, coupled with the establishment of a website branded with the name, can serve as a basis for establishing 'use in commerce' of the trademark.

13 Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

It can. In the US, improper registration of a domain name can be challenged through an arbitral proceeding under the applicable Uniform Domain Name Dispute Resolution Policy (UDRP), or by filing a federal lawsuit under ACPA (see question 2). Under most UDRPs, one must demonstrate:

(i) that the domain name is identical or confusingly similar to a trademark in which the complaining party has rights;
(ii) that the registrant does not have rights or a legitimate interest in the domain name; and
(iii) that the domain name was registered and used in bad faith.

Ownership of a trademark affects factors (i) and (ii), and it also can be used in connection with factor (iii), to show that the registrant knew at registration that the complaining party owned the trademark. The UDRP panel is sometimes willing to recognise ownership of unregistered common law trademark rights, such as in a personal name or nickname.

ACPA assigns liability if one has a bad-faith intent to profit from a mark and 'registers, traffics in, or uses a domain name' that is confusingly similar to a distinctive mark, or is dilutive of a famous mark (15 USC, section 1125(d)(1)(A)(i)-(ii)). As with the UDRP, ownership of a registration supports a plaintiff's ability to demonstrate distinctiveness of his or her trademark, as well as bad faith on the part of the registrant. ACPA potentially offers trademark owners a wider range of remedies (such as money damages), beyond merely cancelling or transferring the domain name under the UDRP policies.

Both UDRPs and ACPA provide non-exhaustive lists of factors to be considered when assessing the possibility of bad faith on the part of the registrant, such as registering a domain name for the purpose of disrupting or diverting the business of a competitor.

Advertising

14 What rules govern advertising on the internet?

Under the FTC Act, FTC is permitted to take all actions necessary to protect consumers from deceptive and unfair acts or practices on the internet. According to the Commission, a representation, omission or practice is deceptive if it is likely to mislead consumers and affect consumers' behaviour or decisions about the product or service. Furthermore, there is a developing set of federal and state laws and regulations concerning electronic advertising, each of which focuses on a particular type of advertising vehicle.

E-mail

The CAN-SPAM Act of 2003, 15 USC, section 7701 et seq (Act) requires that the senders of 'commercial electronic mail messages' meet six basic conditions:

- identify the e-mail as an advertisement or solicitation, in the absence of 'affirmative consent' by the recipient;
- provide notice and return e-mail or other comparable mechanism for recipients to opt out of future e-mails;
- keep return e-mail or other opt-out mechanism active for 30 days;
- honour opt-out requests promptly (within 10 business days of request);
- provide its physical postal address in the e-mail; and
- use accurate header information, descriptive subject liness, originating e-mail addresses, domain names and IP addresses.

Certain state laws augment the CAN-SPAM regulations by, for example, criminalising certain types of 'SPAM' behaviour. However, federal courts disagree as to the extent of CAN-SPAM's pre-emption of state law claims.

Wireless e-mail

In addition to the requirements set forth regarding commercial e-mail, the 'mobile services commercial messages' rules of the CAN SPAM Act require any professional who wishes to send commercial e-mail messages to any type of wireless email address or device, to obtain 'express prior authorisation' (based on the FCC's list of wireless domains or the sender's knowledge). It is permissible to obtain the authorisation either orally or in writing.

In addition to the CAN-SPAM requirements, the Code of Federal Regulation (47 CFR, section 64.3100) places four additional requirements on senders of wireless commercial e-mail:

- include an opt-out mechanism that avoids having the recipient view any additional commercial material;
- include an electronic opt-out mechanism equivalent to the electronic opt-in procedure;
- include a no-charge opt-out mechanism;
- identify itself in a way that the recipient can identify the sender as an authorised entity; and
- companies are thus advised to regularly 'scrub' their e-mail marketing lists against the FCC list of wireless domains to identify wireless recipients.

Short message services (SMS)

The Telephone Consumer Protection Act, 47 USC, section 227 et seq prohibits automatically distributing text messages (commercial or otherwise) without 'express prior consent' of the recipients. Some states have implemented statutes concerning promotional text messaging, which generally require prior consent or a prior relationship, as well as opt-out mechanisms.

Instant messaging (IM)

Although the federal statutes do not currently address IM, several state statutes regarding sending unsolicited bulk e-mail might apply to IM as well.

Besides internet-specific laws, many of the rules that govern advertising in other media, such as federal and state consumer protection laws, apply to advertising on the internet.

15 Are there any products or services that may not be advertised or types of content that are not permitted on the internet?

US internet regulations do not currently address what types of goods or services may be advertised on the internet. In February 2012, however, the current administration released the Consumer Privacy Bill of Rights, outlining principles for how businesses utilise consumer information. The Consumer Privacy Bill of Rights calls for the public and private sectors to work together in developing FTC-enforceable codes of conduct that will guide, among other things, third-party personal data collection for advertising purposes. Likewise, there are generally no regulations that prohibit any particular types of otherwise permissible content on the internet, although actions which would be prohibited offline are also prohibited online. For example, a website service that connects potential room-mates cannot violate the Fair Housing Act, an anti-discrimination statute, by matching users by means of race, sex, family status or sexual orientation. See *Fair Housing Council of San Fernando Valley v Roommates.com*, LLC, 489 F 3d 921 (9th Cir 2007), rev'd in part, vacated in part, aff'd in part, 521 F 3d 1157 (9th Cir 2008) (en banc). Similarly, an internet dating website has recently begun to allow same-sex daters to register for its service as part of a settlement agreement to a discrimination claim. See *McKinley v eHarmony*, DCR Docket No. PQ271B-02846 (12 November 2008 NJ Atty General). In addition, legislation has created an environment where it is very difficult to provide internet gambling services to US residents (see questions 31 to 32). Also, under COPPA (see question 2), sites that target children must take steps before collection of any personal data. Although there is no current prohibition on advertising the availability of prescription drugs without a prescription, the Ryan Haight Online Pharmacy Consumer Protection Act of 2008, 110 P.L. 425, 122 Stat. 4820 prohibits the delivery, distribution, or dispensing of prescription drugs by means of the internet without a valid prescription.

ISPs are generally not liable for the display of prohibited advertisements under the 'Good Samaritan' provision of the CDA (see questions 2 and 17). However, an ISP may be liable if it becomes involved in the creation or substantive modification of the illicit content; see *FTC v Accusearch Inc*, 570 F 3d 1187 (10th Cir 2009) (defendant ISP selling personal data, including telephone records, not entitled to immunity under CDA where it paid researchers to acquire confidential telephone records protected by law). An ISP may also be liable for misrepresentations in its marketing concerning third-party content; see *Mazur v eBay Inc*, 2008 US Dist Lexis 16561 (ND Cal 4 March 2008) (CDA does not shield eBay from plaintiff's complaint that eBay represented tortious third-party vendor as 'safe'). An ISP may not be liable, however, where it is not responsible for affirmatively creating the content that results in the misrepresentations; see *Goddard v Google Inc*, 2008 US Dist Lexis 101890 (ND California 17 December 2008) (dismissing plaintiff's complaint because plaintiff did not allege that Google 'created or developed' the offending advertisements in any respect, but granting leave to amend the complaint to overcome the 'robust' protections of the CDA). Despite the low likelihood of being found liable for the content of such postings under the CDA, recent pressure by state attorneys general has led a major online listing service to voluntarily remove user-generated advertisements of 'erotic services'.

Financial services

16 Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and, if so, by whom and how?

Several federal laws touch upon financial service companies' obligations with regard to consumer data, privacy and communications (see questions 9 and 10, and 23 to 26). As a general matter, the US has strict laws governing the advertising and selling of securities, as set forth in the Securities Exchange Act of 1934 and the rules of the various securities exchanges, while the GLB (see question 2) aims to protect securities customers' private information. The Securities and Exchange Commission has interpreted these rules to require certain disclosures on websites used by companies to provide information to their investors, and has indicated that it will hold companies liable for misstatements on third-party websites linked to the company if the context of the link and the linked information together create a reasonable inference that the company has approved or endorsed

the linked information; see Commission Guidance on the Use of Company Web Sites, Release No. 34-58288 (1 August 2008). Other federal laws regulate additional aspects of financial services, including the Truth in Lending Act, the Fair Credit Billing Act, the Fair Credit Reporting Act, the Equal Credit Opportunity Act and the Electronic Fund Transfer Act.

Defamation

17 Are ISPs liable for content displayed on their sites?

Under the 'Good Samaritan' provision of the CDA (see question 2), the providers and users of 'interactive computer services' may not be 'treated as the publisher or speaker of any information provided by another information content provider'. This means that an ISP is immunised from all liability arising from such content as long as it does not become involved in the creation or substantive modification of content (thus becoming an 'information content provider'). Some courts have declined to extend CDA immunity upon a determination that the defendant party was actively involved in the behaviour at issue.

For example, a website that 'induces' users to violate a law has been found ineligible for the benefit of CDA immunity; see *NPS LLC Inc v StubHub Inc*, 25 Mass L Rep 478 (Mass Super Ct 2009) (website's variable commission rate induced users to resell tickets for prices violating state anti-scalping law). However, a subsequent court has disagreed. The North Carolina Court of Appeals recently criticised the NPS decision, holding that it 'do[es] not find the reasoning employed by NPS persuasive, believe[s] that it is inconsistent with the decisions concluding that knowledge of unlawful content does not strip a website of the immunity from liability granted under 47 USC section 230, and decline[s] to follow it' (*Hill v Stubhub Inc*, 727 SE 2d 550 (NC Ct App 2012). Even if immunised by the CDA, an ISP may be subject to court orders in cases against its users. For example, an evolving body of case law addresses when ISPs must disclose the identity of anonymous internet commentators in defamation cases. See, for example, *Independent Newspapers Inc v Brodie*, 407 Md 415 (Md 2009) (setting out a five-factor test to balance the First Amendment right to anonymity against the right of a plaintiff to seek redress); *Mortgage Specialists Inc v Implode-Explode Heavy Indus.*, 160 NH 227 (NH 2010) (adopting the same test); *Sinclair v TubeSockTedD*, 596 F Supp 2d 128 (DDC 2009) (three-part test for same). The 'Good Samaritan' exception does not extend to criminal violations or to intellectual property liability, although in the case of copyright liability there are separate safe harbours set forth in the DMCA (see questions 2 and 22).

18 Can an ISP shut down a web page containing defamatory material without court authorisation?

The CDA's 'Good Samaritan' provision does not require ISPs to take down any material for which they are immunised, even when placed on notice of the defamatory material. Generally, if an ISP wishes to remove defamatory or other offensive material on its own it may do so. The CDA specifically immunises service providers for any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected (47 USC, section 230(a)(2)(A)).

The 'Good Samaritan' provision was enacted, in part, to encourage voluntary monitoring of content by ISPs without fear of recrimination for errors. An ISP's freedom to edit materials it allows on its sites may even immunise it from claims of antitrust violations; see *LiveUniverse Inc v MySpace Inc*, 304 Fed Appx 554 (9th Cir 2008) (allowing MySpace to censor its users' attempts to include mentions of LiveUniverse, a rival social networking site). Any shutdown should be measured, so as to satisfy the 'good faith' standard set forth above, and in all instances ISPs should check their customer contracts and terms of use before engaging in any monitoring or content removal for relevant provisions. While the CDA's 'Good Samaritan' provision does not require ISPs to take down any material for which they are immunised, an ISP is open to a promissory estoppel claim if it promises to take down third-party tortious content and fails to do so; see *Barnes v Yahoo! Inc*, 570 F 3d 1096 (9th Cir Or 2009).

19 Can a website owner link to third-party websites without permission?

There is no US legislation that prevents one website from linking to another website without permission, although there are circumstances where linking can give rise to liability (see question 22). 'Deep-linking' (linking directly to content within a website, as opposed to the website's homepage) is likewise not prohibited, although this type of linking is met with more criticism and has required website owners to specially program their sites to prevent other websites from providing deep links to their sites. One is also advised to check the terms of use of the target website before linking to it for any provisions addressing linking.

20 Can a website owner use third-party content on its website without permission from the third-party content provider?

This practice is not advisable, as there is a high likelihood of running afoul of the US copyright laws. Generally speaking, one can claim copyright in any creative work fixed in an artistic medium, including all forms of writing on the internet. Copyright protection begins from the moment of creation. Thus, reproducing others' content on one's own website can give rise to claims of copyright infringement. The 'fair use' exception to copyright gives limited protection for certain uses, such as taking excerpts for purposes of commentary, but the application of this exception is necessarily a fact-specific question in every case. The 'fair use' exception has also been extended to the use of thumbnail images as long as the use for the thumbnail image is 'transformative' (used for a different purpose than the purpose of the original image). See *Kelly v Arriba Soft Corp*, 336 F3d 811 (9th Cir 2003) (holding that a search engine's use of thumbnail images in search function did not constitute copyright infringement because thumbnails were used to index and improve access to images on the internet and were not used for aesthetic or commercial purposes because they were much smaller and lower resolution than original images). Fair use continues to be a case-by-case analysis that usually turns on the specific facts of each case. It also continues to be the subject of much controversy and uncertainty in some high profile cases, including the *Google Books* and *HathiTrust* cases (see 'Update and trends'). Recent cases have clarified that the use of third-party trademarks in keyword 'metatags' (information, not visible to a website user, which influences how search engines index the website) is a use in commerce sufficient to state a claim for trademark infringement; see *Rescuecom Corp v Google Inc*, 562 F 3d 123 (2d Cir 2009) and 1-800 *Contacts Inc v Memorial Eye*, PA, 2010 US Dist Lexis 23972 (D Utah 15 March 2010). However, in another recent case, the court found an internet search engine not liable for trademark infringement for selling a plaintiff's trademarked name to a competitor as an 'adword' (a search term that triggers the display of an advertisement); see *Rosetta Stone Ltd v Google Inc*, 730 F Supp 2d 531 (ED Va 2010). A portion of the opinion has been reversed and remanded for further proceedings to address Rosetta Stone's direct and contributory trademark infringement claims, which may disturb the trial court's conclusion that Google has no liability (*Rosetta Stone Ltd v Google Inc*, 676 F 3d 144 (4th Cir 2012)).

21 Can a website owner exploit the software used for a website by licensing the software to third parties?

A provider can exploit software if it is the holder of the underlying intellectual property rights. In the US, software can be protected by both copyright (for the source code) and patent law (for the ideas behind the software).

22 Are any liabilities incurred by links to third-party websites?

Although linking to other websites is generally permitted, it can under certain circumstances give rise to liability. The DMCA includes a limited safe harbour from copyright liability 'for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link' (17 USC, section 512(d)). However, this safe harbour only extends to copyright liability, and is only available if the service provider lacks actual or circumstantial knowledge of the infringing nature of the linked content, does not benefit financially from the infringing activity, and responds expeditiously to notice of the alleged infringement.

Several courts have also recognised that linking, under certain circumstances, can give rise to trademark or copyright liability. For example, links that duplicate or integrate content on a linked page can unintentionally infringe copyrights or trademarks owned by the linked site. See *OBH Inc v Spotlight Magazine Inc*, 86 F Supp 2d 176 (WDNY 2000) (finding trademark infringement when website incorporating plaintiff's name hyperlinked to defendant's online business website); P*eople for the Ethical Treatment of Animals Inc v Doughney*, 113 F Supp 2d 915 (ED Va 2000) (finding 'commercial use' factor satisfied by use of hyperlinks to websites criticising plaintiff's organisation on site with domain name similar to plaintiff's trademark); *Batesville Servs v Funeral Depot Inc*, 2004 US Dist Lexis 24336 (SD Ind 10 Nov 2004)(finding sufficient involvement by defendant in creation of infringing content to potentially give rise to liability by virtue of defendant's hyperlink to such content); *Disney Enters v Showstash.com*, 2008 US Dist Lexis 42642 (CD Cal 20 May 2008) (finding defendant liable under secondary copyright infringement theories for linking to infringing copies of movies and television programmes on other websites). However, courts have held that the mere use of a trademark on a website is not sufficient to create liability. In order to be infringing, the use must be in connection with the sale of goods and services; see *Utah Lighthouse Ministry v Found for Apologetic Info & Research*, (FAIR), 527 F 3d 1045 (D Utah 2008) (finding that merely linking was not sufficient to create trademark liability and that the linking needed to be in connection with the sale of goods and services); Order Granting Motion to Dismiss, *Rosetta Stone Ltd v Google, Inc*, No. 1:09cv736 (28 April 2010) (rejecting assertion that Google's 'sponsored links' triggered trademark liability).

Civil and potentially criminal liability can also arise if one links to information regarding circumvention of copyright protection measures, under the anti-circumvention provisions of the DMCA (17 USC, section 1201); see *Universal City Studios Inc v Corley*, 273 F 3d 429 (2d Cir NY 2001) (affirming injunction against linking to DVD decryption software).

Data protection and privacy

23 How does the law in your jurisdiction define 'personal data'?

Since August 2002, 47 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted data breach notification statutes. Although there are variations among the different state acts, many define personal data as an individual's last name in combination with another data element, such as the individual's social security number.

24 Does a website owner have to register with any controlling body to process personal data? May a website provider sell personal data about website users to third parties?

The US does not require website providers to register with any authority before processing personal data, nor does it generally prohibit website providers from selling personal data about website users to third parties (questions such as this are usually governed by contract). However, the federal government has implemented legislation which restricts the sale or dissemination of specific categories of information including financial information, medical records, video rental history and information about children under 12 years of age. Moreover, under many of the state personal data statutes discussed in questions 23 and 27, website providers are required to notify individuals if their personal data has been compromised by their acquisition by a third party.

25 If a website owner is intending to profile its customer base to target advertising on its website, is this regulated in your jurisdiction? In particular, is there an opt-out or opt-in approach to the use of cookies or similar technologies?

There is no specific US regulation regarding profiling customer bases for advertising purposes, although consumer data are afforded some protection by the Electronic Communications Privacy Act (18 USC 2701 et seq) (ECPA), the Wiretap Act (18 USC 2510 et seq) and the Computer Fraud and Abuse Act (18 USC, section 1030) (CFAA). To date, several courts have dismissed complaints seeking damages for the use of personal information for website advertisement on the basis that 'cookies' are data stored on users' computers, and thus not technically protected under the federal statutes; see, for example, *In re DoubleClick Litig*, 154 F Supp 2d 497 (SDNY 2001) (placement of cookies on plaintiffs' hard drives fell under an exception of the ECPA, as collection of information stored in cookies did not constitute illicit interception of electronic communications under the Wiretap Act, and plaintiffs' damages did not meet the threshold required under the CFAA). In *Lane v Facebook, Inc*, 2009 US Dist Lexis 103668 (ND Cal 2009) a class of Facebook users alleged, inter alia, violations of the Wiretap Act and the CFAA. The users complained that Facebook violated these statutes by automatically publishing information about user purchases from partner websites. The case ultimately reached a settlement agreement (*Lane v Facebook, Inc*, 2010 Lexis 24762 (ND Cal 2010)).

Like profiling customer bases for advertising purposes, the placement of cookies and similar technologies on a consumer's computer for advertising purposes is not specifically regulated by the US and the collection of data through cookies placed on a personal computer falls under an exemption to the Stored Communications Act (see question 2); 18 USC section 2701; see *In re Toys 'R' Us Inc*, Privacy Litig, 2001 US Dist Lexis 16947 (ND Cal 2001) (holding that cookies are not electronic storage under the Stored Communications Act). There is thus, as yet, no uniform opt-in or opt-out approach in connection with cookies and the like (but see 'Update and trends').

26 If an internet company's server is located outside the jurisdiction, are any legal problems created when transferring and processing personal data?

As stated, there is no comprehensive privacy legislation at the federal level. The US and the EU have put in place a safe harbour programme by which US organisations can be certified to transfer data to the EU without running afoul of the EU Privacy Directive. With effect from 1 March 2009 there is a registration requirement and annual fee for the use of this safe harbour programme. Failure to satisfy the safe harbour potentially exposes US firms to liability for international data transfers. Currently, the US and the EU are negotiating to develop a data privacy and protection agreement balancing individual privacy protection with data exchange for

crime and terrorism-fighting purposes. Additionally, maintaining a server in a particular location could have an impact on personal jurisdiction, should litigation be commenced in that jurisdiction (see question 4).

27 Does your jurisdiction have data breach notification laws?

As discussed in question 23, almost every state has enacted a data protection statute. The federal government has yet to enact any data breach laws with national coverage. These statutes provide for rapid consumer notification of a breach of data security. The majority of states require notification of consumers whose personal data were compromised to occur at the 'most expedient time possible, without unreasonable delay'. Most of the states exempt breaches that expose encrypted data from the notification rule. Many states also exempt breaches which expose data that are made publicly available by government entities.

Taxation

28 Is the sale of online products subject to taxation?

Most states have tax exemptions on certain items, such as food or clothing. However, with the exception of Alaska, Delaware, Hawaii, Montana, New Hampshire and Oregon, that do not have a sales tax, the sale of online products can be subject to a sales tax if the seller has a taxable nexus to the buyer's jurisdiction. Such a taxable nexus is created by, for example, a store or warehouse located in the state or a contractual relationship with an in-state affiliate. Sales taxes, imposed by a state or local jurisdiction, vary widely in both the level of the tax and the products to which they apply. Recently, states have passed laws or interpreted existing law to create a 'click-through nexus' for online retailers who have a contractual agreement with an in-state resident under which the in-state resident refers customers to the online retailer for some form of consideration. However, the Marketplace Fairness Act of 2013, which was approved by the US Senate in May 2013 and is supported by the Obama administration, will modify the nexus requirement if the Act is approved by the US House of Representatives. The Marketplace Fairness Act would permit the 45 states and the District of Columbia that currently charge sales tax to require all online retailers who have sales of at least $1 million outside of states where they have a physical presence to charge sales tax on purchases made by their residents. While there is no federal sales tax, since 2011 the Housing and Economic Recovery Act of 2008 has required all processors of online payments to report merchants' annual gross receipts to the Internal Revenue Service for federal income tax purposes. Since the enactment of the Internet Tax Freedom Act in 1998 (47 USC, section 151 note), there has been a moratorium on any new taxes on internet access or 'multiple or discriminatory taxes on electronic commerce'. In 2007 that moratorium was extended to 1 November 2014, and a bill was recently introduced in the Senate to make the moratorium permanent.

29 What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Usually if a business owns a server in a US state outside its home jurisdiction, that ownership is sufficient to establish a taxable nexus that will allow the state and local jurisdictions to tax any sales in that state. Certain states, such as Vermont, have specific exemptions for this situation and do not consider the presence of a server in the state to be a taxable nexus (32 VSA, section 5811(15)(c)(2)). Several states, including California, Oklahoma, New York and Texas have adopted regulations or issued legal rulings to clarify that a taxable nexus is not created when an out-of-state company uses an in-state computer, which it does not own, to host its website or transact e-commerce.

30 When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

There is no VAT in the US. Sellers are required to collect sales taxes from buyers in jurisdictions where the seller has a taxable nexus (see question 28).

31 If an offshore company is used to supply goods over the internet, how will returns be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

Goods that are returned for a refund should, generally, not affect a supply company's tax liability. Transfer-pricing problems may arise from customers returning goods to an onshore branch of an offshore company if the transfer price from the offshore company to the onshore branch for that particular good is much higher than the price the customer paid in the online sale, as it might be viewed as evidence that the transfer price was unreasonably high and thus not result in a deduction of the full amount.

Gambling

32 Is it permissible to operate an online betting or gaming business from the jurisdiction?

The legality of online gambling in the US depends on where both the operator and the bettor are located. Approximately 10 states in the US have outlawed online gambling entirely and many others restrict it. The Federal Wire Act (18 USC, section 1084) prohibits all forms of sports betting and UIGEA (31 USC, section 5361–67 et seq), passed in October 2006 (see question 2), prohibits certain financial transactions related to proscribed gambling activities. UIGEA has led to many online gambling sites discontinuing service to US players. By contrast, the proposed Internet Gambling Regulation, Consumer Protection, and Enforcement Act of 2013, introduced in the US House of Representatives, would legalise online gambling. The proposed Internet Gambling Regulation and Tax Enforcement Act of 2011 would have taxed internet gambling, but it was not passed.

33 Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

Whether residents are permitted to use online casinos or betting websites depends on the state in which they will use those websites. As discussed above, some states have outlawed online gambling entirely. Those states that allow it are responsible for regulation of age, credit and other requirements. Recent high-profile law enforcement actions against online gambling sites have spurred the House of Representatives to introduce legislation which would allow for the closer regulation of online poker while exempting online poker from the restrictions of the UIGEA mentioned in question 32.

Outsourcing

34 What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

Some of the key legal and tax issues relevant to outsourcing include the enforceability of contractual choice of law and forum provisions in the offshore jurisdiction; enforcement of intellectual property, employment, and property laws even when these areas are covered by the terms of the contract; and compliance with applicable US legal, regulatory and accounting requirements, such as HIPAA, GLB (see question 2) and the Sarbanes-Oxley Act. Increasing attention is being paid to the Foreign Corrupt Practices Act (FCPA) (15 USC, sections 78m(b)(2)-(3), 78dd-1, 78dd-2 and 78ff), which can subject companies to US litigation and liability for corruption taking

Update and trends

A key set of issues that continue to receive substantial attention in the US relate to the potential liability of companies that make use of others' copyrighted works on the internet. In recent years, two cases have received particular prominence – the *Viacom International Inc v YouTube Inc* litigation (2007 Civ 2103) in New York, and the *UMG Recordings Inc v Shelter Capital Partners LLC* case (09-55902) in California, which began in 2007 and 2009, respectively, both of which have now concluded. In the *Viacom* case, the trial court judge in the Southern District of New York granted summary judgment to *YouTube* on 23 June 2010, ruling that YouTube had no direct or secondary copyright liability for videos posted by users, because YouTube had adhered to the 'notice and takedown' procedures of the Digital Millennium Copyright Act (DMCA) (see questions 2, 17 and 22). On 4 April 2012, in the Second Circuit Court of Appeals (10-3270), the appeals court disagreed with the trial court on the interpretation of certain provisions of the DMCA, as well as the lower court's application of the DMCA to the facts of the case, and remanded the case to the district court for further analysis, centering on YouTube's potential responsibility to act in the face of awareness of infringing activity. On 18 April 2013, however, the district court granted summary judgment again to YouTube, concluding that the issues it was instructed to revisit did not change the outcome of the case. While Viacom originally filed papers initiating another appeal in its case against YouTube, in December 2014 that appeal was withdrawn, signaling that the case had been settled. In the *UMG* case in California, the district court granted the defendant's motion for summary judgment on 11 September 2009, and the Ninth Circuit Court of Appeals affirmed most of that decision on 20 December 2011. After the Second Circuit's decision in *Viacom* in 2012, however, the Ninth Circuit invited the parties to submit supplemental briefs focusing on the potential impact of the *Viacom* decision on the *UMG* case. On 14 March 2013, the Ninth Circuit issued a replacement opinion that reached the same conclusions but also discussed the Second Circuit's *Viacom* decision. The April 2013 decision in the *Viacom* case in turn made references to the Ninth Circuit's March 2013 decision. Although both Courts of Appeal sided with the defendants in their respective cases, the Copyright community continues to speculate and debate whether and the extent to which the two Circuit Courts in fact agreed or disagreed as to the finer points of the interpretation of the DMCA, which could have far-reaching impact beyond these two cases.

Another high-profile pair of cases relate to the Google Books project, under way since 2005, where Google has been scanning books at several cooperating university libraries and posting the results to a searchable database on the internet. *The Authors Guild v Google Inc* (05 Civ 8136), pending in the Federal District Court for the Southern District of New York, was brought by groups of book authors and publishers against Google on the claim that the Google Books project violates their copyrights. The second case, *The Authors Guild v Hathitrust* (11 cv 6351), also pending in the Southern District of New York, focuses on the university libraries and the Hathitrust service created by the libraries, and their provision of digital copies of the scanned books to various classes of patrons. After six years of litigation, the *Google* case initially resulted in a large class action settlement, on 22 March 2011 the trial judge rejected the settlement for a number of reasons, explaining generally that it was not 'fair, adequate, and reasonable', and suggesting that a central flaw of the settlement is its 'opt-out', versus 'opt-in', structure. The *Google* case then resumed its course, with the District Court granting class certification, and the parties submitting briefs on the question of whether the scanning was a fair use under the Copyright Act. In the *Hathitrust* case, on 10 October 2012, the District Court sided with the defendants on the various motions before the court, finding that the particular activities of the defendants qualified for the fair use defence under the Copyright Act. Then, on 1 July 2013, the Second Circuit reversed the District Court's grant of class certification in the *Google* case, and directed the parties to litigate the question of fair use first. After completing briefing on the fair use question, the District Court judge in the *Google* case concluded that Google also enjoys a complete fair use defence. That decision is now on appeal to the Second Circuit Court of Appeals. Oral argument has yet to be scheduled. In June 2014, however, the Second Circuit Court of Appeals issued a ruling upholding the lower court's fair use decisions in the *Hathitrust* case, leading to speculation about whether the appeal in the *Google* case will follow a similar course, or if there is room for divergent opinions on the issue.

One more very high-profile group of cases has been brought by the major broadcast television networks against Aereo, a company that streams television content over the internet without the consent of the broadcasters, using technology designed to avoid liability under the Copyright Act, based largely on a prior decision by the Second Circuit Court of Appeals involving a 'remote DVR' system (*Cartoon Network LP, LLLP v CSC Holdings, Inc*, 536 F.3d 121 (2d Cir 2008)). Following rulings in favour of Aereo at the District Court and Court of Appeals (but some decisions to the contrary in other US courts), the case has been accepted for appeal to the United States Supreme Court, with a decision expected in June 2014. See *American Broadcasting Companies v Aereo, Inc, f/k/a Bamboom Labs, Inc* (13-461).

In another area of e-commerce, there is a growing trend toward promoting employee and applicant social networking privacy. Forty-four states and the federal government have introduced legislation making it illegal for employers or potential employers to request social media passwords from employees, force employees to access social media accounts or indirectly access employee social media accounts through third parties. In fact, 13 states have already passed laws making it illegal for employers to request social media passwords from employees or candidates.

place overseas. Prohibited conduct worldwide can be subject to FCPA rules. In addition, according to US Securities and Exchange Commission, the act applies to publicly traded companies and their officers, directors, employees, stockholders, and agents. Agents can include third party agents, consultants, distributors, joint-venture partners and others.

35 What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, do the rules apply to all employees within the jurisdiction?

Other than federal anti-discrimination laws, most employment law in the US is regulated by state and local entities. Therefore, unless firing of domestic employees in favour of foreign-based outsourced employees can be shown to implicate discrimination against a protected class, or specific contract rights, the former employees are unlikely to be able to maintain any type of federal employment action. The federal Worker Adjustment and Retraining Notification Act (29 USC, section 2101 et seq) (WARN Act), requires employers with 100 or more full-time employees (not counting those who have worked less than six months in the past 12 months), to give notice 60 days in advance of any layoff that affects a certain number or percentage of workers, and thus in those circumstances the soon-to-be-terminated employees would have opportunity to seek alternative employment. The federal WARN Act is supplemented by similar legislation imposing additional regulations in more than 15 states. The House of Representatives has voted down two separate bills that would have discouraged employers from outsourcing jobs to foreign countries (HR 3596: United States Call Center Worker and Consumer Protection Act; HR 3875: Outsourcing Accountability Act of 2012).

Online publishing

36 When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability?

Generally speaking, errors in online data can open up a website provider to the same liabilities that arise from such mistakes in print media and the like, although the particular circumstances would dictate what type of liability, and what type of damages (if any) might be available. As discussed above, this only applies if the website provider is the provider of the content. If the website provider

is a passive host of content provided by someone else, it will often find complete immunity under the 'Good Samaritan' provision of the Communications Decency Act (see questions 2, 15, 17 and 18). A recent case has clarified that the online auction site eBay is not liable as a provider or publisher of content when third parties use its service to sell counterfeit, trademark-infringing goods; see *Tiffany (NJ) Inc v eBay Inc*, 576 F Supp 2d 463 (SDNY, 2008) aff'd in part, rev'd in part, 600 F 3d 93 (2d Cir 2010). However, the court in *Tiffany v eBay* noted that if eBay had reason to know that trademark infringement was occurring on their site and if they had continued to allow that infringing content on their website, then eBay could be found contributorially liable.

37 If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

Databases that contain a minimum level of originality and creativity enjoy protection under US copyright law, limited generally to the arrangement and presentation of the data, rather than the underlying data themselves. See 17 USC, section 103b. If the provider of a website wished to protect itself from unauthorised reproduction of data, it could consider limiting access to the site by licensing the data or placing restrictions in the terms of use of the site. A 'click through'-type model can be used to ensure affirmative consent to these terms of use before users obtain access to the data themselves.

38 Are there marketing and advertising regulations affecting website providers?

The same consumer protection laws that apply to commercial activities in other media also have application online. The FTC Act's prohibition on 'unfair or deceptive acts or practices' (see question 2) encompasses internet marketing and advertising. In addition, many FTC rules and guides are not limited to any particular medium used to disseminate claims or advertising and, therefore, apply to online activities. Online advertising must be truthful, substantiated and fair. Misleading advertising is prohibited. Advertisers must identify all express and implied claims that the advertisement conveys to consumers. If an advertisement makes express or implied claims that are likely to be misleading without certain qualifying information, the information must be disclosed. Disclosures that are required to prevent deception or to provide consumers material information about a transaction must be presented 'clearly and conspicuously'. See *US v Locascio*, 357 F Supp 2d 536, 548–49 (EDNY 2004). A disclosure cannot cure a false claim. Thus, if a disclosure provides information that contradicts a claim, the disclosure will not be sufficient to prevent the advertisement from being deceptive. Unique features in internet advertisements may also affect how an advertisement and any required disclosures are evaluated.

The FTC also monitors the internet for advertisements, in any form, that seek to mislead consumers, for example by making unsubstantiated claims about the health benefits of a product, or by using testimonials or endorsements that do not reflect typical experiences of consumers.The application of these types of statutes to e-commerce is an evolving area of law. For example, a recent civil suit tested whether mail and wire fraud statutes can be used to stop 'click fraud', where a person, automated script or computer program repeatedly clicks on an online advertisement, generating additional charges for the advertiser (see *Microsoft v Lam*, 09-cv-0815 (complaint filed 15 June 2009 WD Wash)), and resulted in the imposition of a permanent injunction against the defendants in 2010. In 2009, the FTC published guidelines for online behavioural advertisements, which track consumers' online activities in order to deliver tailored advertising (see Federal Trade Commission, Self Regulatory Principles for Online Behavioural Advertising). The FTC has proposed the implementation of a 'do not track' mechanism to allow internet users to opt out of behavioural advertising. The Do Not Track Online Act of 2013, if successful, will mandate all websites that collect personal data to provide a 'do not track' option. Meanwhile, the Digital Advertising Alliance has implemented a self-regulatory opt-out programme which gives consumers the choice to opt-out of behavioural advertisements from the 131 companies that currently participate in the programme. Additionally, the FTC is in the process of revising its Dot Com Disclosure guidelines, which were initially issued in 2000 and offer guidance to businesses about the application of federal advertising law to internet advertising and sales.

In addition to the FTC Act, other federal statutes mandate requirements for certain types of online advertisements. For example, all forms of advertising for pharmaceuticals are regulated by the Food and Drug Administration, which has recently moved to enforce the inclusion of risk information about drugs in search advertisements (the short text advertisements appearing beside search engine results).

Various state laws may also apply to internet advertising. In New York, for example, the state legislature will consider whether to enact the Internet Online Consumer Protection Act, which if passed would oblige companies to allow consumers to opt out of being targeted based on their behaviour, and also require consent before personal information can be collected.

* *The author would like to thank Natalina DePina (Boston College Law School, JD expected May 2016), a 2014 summer associate at Robins, Kaplan, Miller & Ciresi LLP, for her invaluable assistance and contributions to the 2015 edition of this chapter.*

Parness Law Firm, PLLC

Hillel I Parness **hip@hiplaw.com**

136 Madison Avenue, 6th Floor
New York, NY 10016
United States

Tel: +1 212 447 5299 or 646 526 8261
Fax: +1 646 722 3301
www.hiplaw.com

E-COMMERCE 2015 ISSN 1473-0065