e-Commerce

Contributing editor
Robert Bond

2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

e-Commerce 2018

Contributing editor
Robert Bond
Bristows LLP

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.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 3708 4199
Fax: +44 20 7229 6910

First published 2000
Fourteenth edition
ISSN 1473-0065

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

CONTENTS

United States

Gregg Kirchhoefer, P Daniel Bond, Ashley Eisenberg and Adine Mitrani
Kirkland & Ellis LLP

General

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

Addressing internet issues is a key priority for the US government, which has recognised the criticality of the internet to economic growth and the creation of jobs. The US government has demonstrated its commitment to ensuring and fostering the growth of the internet economy in myriad ways over the past few years. In particular, the US government has focused on initiatives, policies and engagements that are aimed at ensuring that the internet remains open and free, and protecting cyberspace and improving data security.

As to access to the internet, in 2009, the US government earmarked US$7 billion in investments from the Recovery Act to expand broadband access through the US, to improve high-speed internet connectivity in rural areas, and to increase internet capacity in community buildings. Further, in March 2016, the Federal Communications Commission (FCC) approved rules to modernise 'Lifeline' (the FCC's programme to help make communications services more affordable for low-income consumers) so that subscribers can purchase discounted broadband from participating providers. Under the Trump administration, FCC Chairman Ajit Pai has reformed Lifeline and rolled back some the recent regulations promulgated by his predecessor, Tom Wheeler of the Obama administration. In February 2017, the FCC blocked nine companies from participating in the programme, and in March 2017, the FCC announced that states would set eligibility criteria to select broadband providers for the programme.

With respect to US government initiatives to ensure that the internet remains open and free, in July 2011, at the Organisation for Economic Co-operation and Development, the Obama administration affirmed the Internet Policy Making Principles that aim, among other things, to promote and to protect the global free flow of information. In addition, in 2015, the FCC voted in favour of a robust net neutrality rule to keep the internet open and free. The US Commerce Department Office of the Secretary also created an Internet Policy Task Force to carry out a review of the nexus among privacy policy, copyright, global free flow of information, cybersecurity, and innovation in the internet economy to identify internet-related public policy and operational challenges. Net neutrality rules may not disappear entirely under the Trump administration, but the FCC may be more restrained in enforcing them. In March 2017, President Trump signed a bill repealing internet privacy regulations promulgated last year by the FCC that would have given internet users greater control over what service providers can do with their data.

The US government has also recognised the increasing importance of cybersecurity. Commenting on US cybersecurity infrastructure in 2009, President Obama stated that the 'cyber threat is one of the most serious economic and national security challenges we face as a nation' and that 'America's economic prosperity in the 21st century will depend on cybersecurity.' To this end, the Obama administration implemented the National Strategy for Trusted Identities in Cyberspace aimed at reducing cybersecurity vulnerabilities and improving online privacy protections through the use of trusted digital identities. In 2011, the Obama administration also released the International Strategy for Cyberspace to assure the free flow of information, the security and privacy of data and the integrity of the digital infrastructure. In December 2015, the Cybersecurity Act was passed, which provides important tools to strengthen cybersecurity in the US, particularly by expanding the power of network operators to conduct surveillance for cybersecurity purposes. In August 2016, a three-judge Ninth Circuit panel interpreted the exemption of common carriers from Federal Trade Commission (FTC) oversight in such a way that blocks the FTC from policing anticompetitive, unfair and deceptive practices.

The future of internet policy is uncertain under the Trump administration. However, the general trend has been less stringent FCC policing and fewer regulations. Under the Trump administration, Congress has already rolled back Obama-era FCC privacy regulations for broadband service providers.

The US government under the past several administrations has recognised the importance of the internet as a platform for commerce, innovation and education, and has identified ways in which to ensure that the internet is widely available, fair and safe, and has aggressively legislated to adapt to the rapidly evolving internet environment.

Legislation

2 What legislation governs business on the internet?

In addition to state laws, the US has numerous federal laws that address various aspects of conducting business on the internet. These laws include measures that regulate, among other things, the use of personal information, advertising, intellectual property, business and speech in cyberspace. Some of the key laws regarding the foregoing are set out below:

- The Online Copyright Infringement Liability Limitation Act of the Digital Millennium Copyright Act of 1998 (DMCA) creates a framework of safe harbour provisions and procedural requirements that, in certain circumstances, insulate internet service providers (ISPs) from copyright infringement claims based on actions by users of their services where a copyright owner has provided notice of the alleged copyright infringement to the ISP.
- The Federal Trade Commission Act of 1914 (FTCA) broadly prevents unfair methods of competition and unfair or deceptive acts or practices affecting interstate commerce. The FTCA applies to advertising on the internet.
- The Gramm-Leach-Bliley Act of 1999 (GLBA) regulates the collection, use, protection and disclosure of non-public personal information by financial institutions.
- The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the CAN-SPAM Act) governs unsolicited email communications and, among other things, prohibits false or misleading email header information and deceptive subject lines, requires certain information to be disclosed in email communications, and requires senders to provide recipients with a way to opt out of receiving future email communications.
- The Children's Online Privacy Protection Act (COPPA) governs the online collection of personal information from children under the age of 13. More specifically, COPPA applies to companies with websites and online services that are directed at children under the age of 13 and have actual knowledge that they are collecting information from children under the age of 13.
- The Health Insurance Portability and Accountability Act (HIPAA) governs individually identifiable health information and applies

broadly to healthcare providers, data processors, pharmacies and other entities that handle information, and sets out standards that apply to the electronic transmission of medical data.

- The Electronic Communications Privacy Act (ECPA) governs the interception of electronic communications and applies to anyone who improperly accesses, intercepts or discloses electronic communications that affect interstate or foreign commerce.
- The Computer Fraud and Abuse Act (CFAA) governs computer hacking and makes unlawful certain computer-related activities involving the unauthorised access of a computer without authorisation.
- The Restore Online Shopper's Confidence Act (ROSCA) places restrictions on third-party data passing, which occurs when one company (the 'initial merchant') passes along its customers' billing information to a third-party company that may then charge such customers for goods or services that they did not consent to purchase. Under ROSCA, a third-party seller is prohibited from charging a consumer for any goods or services sold on the internet unless it has disclosed clearly all material terms of the transaction, and has obtained the consumer's express informed consent to the charge. Although initial merchants are prohibited from disclosing to third-party sellers any billing information used to charge consumers post-transaction, this provision does not extend to subsidiaries, corporate affiliates or successors to the initial merchant.
- The Communications Decency Act of 1996 (CDA) regulates the distribution of obscene content on the internet and provides certain protections to online service providers. The 'Good Samaritan' provision protects online service providers from liability for restricting access or giving others the technical means to restrict access to certain materials.
- The Anticybersquatting Consumer Protection Act of 1999 (ACPA) creates a civil cause of action for owners of trademarks and service marks against a person who (i) registers, traffics in or uses a domain name that is identical or confusingly similar to the mark, or (ii) in the case of a famous mark, dilutes the mark and has a bad faith intent to profit from the use of the mark.
- The Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) regulates online gambling. The UIGEA 'prohibits gambling businesses from knowingly accepting payments in connection with the participation of another person in a bet or wager that involves the use of the Internet and that is unlawful under any federal or state law.'
- The Keeping the Internet Devoid of Sexual Predators Act of 2008 (the KIDS Act) requires sex offenders to provide to the National Sex Offender Registry all internet identifiers used by such offenders and allows social networking sites to search their users for matches in the Registry.
- The Broadband Data Improvement Act of 2008 (BDIA) is aimed at improving the quality of data regarding the availability and quality of broadband services to promote the availability of broadband internet.
- Article 2 of the Uniform Commercial Code (UCC) applies to all contracts (including those concluded online), both business-to-business and business-to-consumer, for the sale of goods. Common law, however, governs contractual transactions related to, inter alia, real estate, services, insurance, intangible assets and employment.
- The FCC Open Internet Rules established 'net neutrality' (ie, measures to maintain open, uninhibited access to online content without internet access providers being allowed to establish fast and slow lanes to content). Although the Trump administration has recently criticised net neutrality rules, it may not be able to substantively roll back the underlying policy behind such rules.
- The Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO IP) increases both civil and criminal penalties for trademark, patent and copyright infringement, including online infringement.
- The Jumpstart Our Business Startups (JOBS) Act: Title III – Crowdfunding regulations permit companies to offer and sell securities through crowdfunding.

It is important to note that while the above list highlights many federal laws, there are numerous other regulations, intellectual property and other laws, state laws and industry standards that are applicable to conducting business on the internet. Further, to the extent US-based websites are aimed at consumers outside the US, the law of foreign jurisdictions may also apply. For example, certain provisions of the European General Data Protection Regulation (GDPR), which will be implemented in May 2018, will apply to businesses if they offer goods or services to data subjects in Europe or monitor data subjects' behaviour in Europe. Additionally, the GDPR establishes a new legal framework for transatlantic transfers of data, called the 'Privacy Shield,' which will replace the US-EU Safe Harbour.

Regulatory bodies

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

The FTC regulates e-commerce activities, including online advertising and consumer privacy. The FTC has historically been the most active government agency overseeing data security and privacy. Since 2002, the FTC has brought more than 60 enforcement actions under Section 5 authority for alleged 'unfair' or 'deceptive' data security practices.

The FCC regulates interstate and international communications by radio, television, wire, satellite and cable, including telecommunications across the internet. Current FCC Chairman Ajit Pai proposes reversing his predecessor's reclassification of the internet as a regulated public utility under Title II. If the FCC approves this proposal, the deregulation of internet providers as Title I information services would prevent the FCC from mandating 'net neutrality' rules subjecting providers to greater regulatory oversight, and would also relinquish the Commission's oversight authority over interconnection agreements between internet providers and edge providers (ie, content companies, including e-commerce sites).

The Federal Financial Institutions Examination Council prescribes uniform principles, standards and report forms for the federal examination of financial institutions and makes recommendations to promote uniformity in the supervision of financial institutions.

The Advisory Commission on Electronic Commerce was created by Congress to study federal, state and local and international taxation and tariffs on transactions using the internet and internet access.

The National Institute of Standards and Technology (NIST), an agency under the Commerce Department, published the NIST Cybersecurity Framework, which has become a widely adopted foundational strategy across most federal agencies. NIST's role in the e-commerce space includes collaboration with the private sector to ensure infrastructure security, as well as co-funding programmes aimed at advancing e-commerce technologies.

Businesses should also consider other government agencies with regulations related to e-commerce, internet access, tariffs and charges (eg, Securities and Exchange Commission (SEC), Office of the Comptroller of Currency and state tax authorities).

In addition to the regulatory bodies listed above, there are state and local regulatory bodies that are responsible for the regulation of e-commerce. Further, certain industries publish guidelines that members are required to adopt. For example, the Direct Marketing Association requires its member to adopt authentication systems for outgoing emails. As another example, the Better Business Bureau (BBB) expects that business partners conduct their business in line with the BBB Business Partner Code of Conduct, which includes requirements with respect to safeguarding data online (including the requirement to disclose a website privacy statement). Furthermore, the popularity of Internet of Things (IoT) devices has had a significant disruptive impact on the e-commerce sector (eg, the Amazon Dash Button). With the recent wave of cyberattacks exploiting cybersecurity weaknesses prevalent among such connected devices, several industry working groups have responded by proposing standardised frameworks targeting IoT security, including the Online Trust Alliance ((OTA) including Microsoft, Symantec, and Verisign) and the Industrial Internet Consortium ((IIC), including AT&T, GE, and IBM). Underwriters Labs (UL) also recently began testing and certifying products according to its UL 2900 series, an IoT cybersecurity standard.

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?

In the US, the general rule is that a defendant company may be sued in the jurisdiction in which the company is incorporated (or for an individual, where he or she resides). Personal jurisdiction is the concept that a defendant should not be subject to a decision of an out-of-state court without having 'purposely availed' itself or him or herself of the benefits of the relevant state. There is an increasing body of US law that helps courts determine when internet activity creates personal jurisdiction over parties. Personal jurisdiction cases frequently involve website owners that advertise their business in many states, but reject the jurisdiction of a particular state on the basis that they do not have sufficient connection with the state to be subjected to the courts of that state. There is currently no Supreme Court precedent, but a number of federal court decisions articulate the circumstances in which personal jurisdiction may be asserted in an internet context. Certain courts distinguish between active and passive websites, such that they will extend jurisdiction over a website proprietor that actively markets to customers in a particular jurisdiction, but not over a passive website that does not purposefully interact with individuals in a particular jurisdiction.

The traditional test of personal jurisdiction arose out of the *International Shoe v Washington US Supreme Court* case, which held that for a defendant to be sued in court in a particular jurisdiction it must have at least a 'minimum level of contact' with the state that it could reasonably expect to be sued in the courts of that state.

Some courts apply the *Calder* effects test from *Calder v Jones* in circumstances where there is insufficient interactivity or minimum contacts, but where a defendant's actions are targeted at a particular forum. The *Calder* effects test requires an intentional action, that was expressly aimed at the forum state, with knowledge that the brunt of the injury would be felt in the forum state. If the defendant's actions meet the test, then personal jurisdiction may be asserted based on internet activities that would not otherwise meet the interactivity of minimum contacts needed for personal jurisdiction.

Several courts look to the 'sliding scale' or *Zippo* test from *Zippo Manufacturing Co. v Zippo Dot Com, Inc.*, in which a district court held that 'the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the internet. This sliding scale is consistent with well-developed personal jurisdiction principles.' Most courts using the *Zippo* test do not regard it as dispositive, and instead view it as a useful guideline for website interactivity in the due process inquiry.

Further cases assist in providing guidance in specific circumstances. For example, in *Pres-Kap, Inc. v System One, Direct Access, Inc.*, the district court held that the remote use of a server physically located in a forum state was insufficient to establish minimum contacts. In *CompuServe, Inc. v Patterson*, the appellate court held that, among other things, selling software through a company's online service was enough to establish minimum contacts in the state where that company was located. In *Cybersell, Inc. v Cybersell, Inc.*, the district court held that a passive web page that did not advertise in Arizona was not enough to establish personal jurisdiction in Arizona. Similarly, the district court in *Acushnet Co. v Zimventures, LLC* held that interactive websites allowing customers to search for sales representatives and store locations in Massachusetts are insufficient to meet the *Zippo* test where it is unclear to what extent that search tool is actually used by Massachusetts customers. Another district court has further emphasised in *Broad. Mktg. Int'l, Ltd. v Prosource Sales & Mktg., Inc.* that the unilateral acts of a third party bringing in the defendant company's advertising or products into the forum state cannot be sufficient to exercise personal jurisdiction, if the defendant company did not anticipate entering the forum state. Notably, each state may have specific rules for personal jurisdiction and these must be carefully considered in each case.

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?

Contracts formed over the internet are formed in the same manner as contracts formed via more conventional means: there must be an offer and acceptance. In the context of electronic contracts, the enforceability of contractual terms generally turns on the question of assent. Traditional contract law recognises that assent can be either express (ie, an unambiguous manifestation of assent) or implied (ie, the implication of assent by the conduct of a counterparty). However, in the context of internet-based contracts, courts to date have proven far more sceptical in addressing implied consent than express consent, particularly in cases where a party is attempting to enforce onerous terms.

'Click-wrap' agreements are typically the easiest to form and enforce. In a click wrap contract, a user of a website is required to expressly assent to terms provided by a website or web service by clicking a button located in close proximity to an express request that a user accept the proposed terms. In many cases, a site may require a user to either scroll through the proposed terms or to check a box affirming that he or she has reviewed those terms prior to clicking the accept button. These sorts of agreements have been routinely enforced by both state and federal courts, so long as the text makes sufficiently clear that a user is accepting a contract. By contrast, the enforceability of so-called 'browse wrap' agreements varies widely on a case-by-case basis. In a browse wrap agreement, a website or web service will post the terms and conditions of use on its website (typically accessible by a hyperlink at the bottom of the page) but does not expressly require a user to click an accept button. In *Sprecht v Netscape*, Second Circuit judge (and current Supreme Court Justice) Sonia Sotomayor ruled that a browse wrap agreement was unenforceable against a user that clicked a button marked 'download' because the link to the terms of the proposed browse wrap agreement was located down the page from the download button and the user was not required to affirmatively indicate his or her acceptance of those terms. This emphasis on reasonable notice and affirmative consent has been mirrored by numerous courts in the US in cases like *Nguyen v Barnes & Noble, Inc.* and *In re Zappos.com, Inc. Customer Data Security Breach Litigation.*

Notably, the scepticism shown by a court in the context of browse wrap agreements is often proportional to how onerous the proposed terms will be on a counterparty. For example, courts are typically much more reticent to enforce mandatory arbitration clauses in the context of browse wrap agreements. *Schnabel v Trilegiant Corp*. Nonetheless, courts will enforce browse wrap agreements in cases where a counterparty acknowledges that it was aware of the terms at the time it began using a website or web service. *Register.com, Inc. v Verio, Inc.* Similarly, courts appear to be more liberal in enforcing browse wrap agreements against sophisticated businesses, particularly where a website includes prominent links to proposed conditions or a website sends communications specifically directing a user's attention to such terms. *Ticketmaster Corp. v Tickets.com, Inc.* However, courts typically closely scrutinise such agreements in the context of consumer cases, as evidenced by rulings like *Hines v Overstock.com, Inc.* and *Kwan v Clearwire Corp.*, barring evidence of express assent or knowledge of the terms by a defendant. This is also true for click wrap agreements; in *Bragg v Linden Research, Inc.* the Californian court held that, even though the plaintiff had clicked the 'accept' button on the terms of service notice before accessing the game Second Life, it was a contract of adhesion and therefore procedurally unconscionable to enforce. The court's reasoning was based on a finding that there was no reasonable alternative similar to Second Life on the market, and that the plaintiff was in a much weaker bargaining position relative to Second Life, resulting in an unconscionable 'take it or leave it' situation.

In cases where an electronic contract does not fit squarely within either a click wrap or a browse wrap agreement, some courts have indicated greater willingness to find the notice necessary for constructive consent where the contract most closely resembles a click wrap agreement. For example, in *Fteja v Facebook, Inc.* the New York District Court found that the agreement between Facebook and its users resembles a click wrap because the user must click 'Sign Up' to assent to Facebook's terms, but also resembles a browse wrap because those terms were only visible by clicking on the hyperlink for 'terms of service'. In that case,

the court held that the agreement was still enforceable, even though the terms of use appeared on a separate page, primarily because Facebook gave users notice of the consequences of clicking 'Sign Up' and clearly directed them to where they could learn about them.

In order to ensure the enforceability of electronic contracts, companies should always employ certain best practices. First, users should not be permitted to access a website or web service until they complete a form requiring them to review and expressly consent to proposed terms of service. Second, websites should not permit a user to click an 'I Accept' button until a user has been forced to either scroll through the proposed terms of service, or to check a box indicating that he or she has reviewed the same via a link in direct proximity of that box. Customers should be provided with reasonable notice and an opportunity to review the company's terms, especially if the electronic agreement in question is a hybrid between click wrap and browse wrap. Third, a user should be required to confirm that he or she is authorised to contractually bind the user by clicking on an additional box to ensure the enforceability of a click wrap agreement. Fourth, it is important for websites to confirm that they have a valid email address on file. This enables companies both to confirm the identity of their users and also to remain in periodic contact with users, including when terms of service change. Fifth, if a particular company's service or product is one-of-a-kind in the market, it should take particular care in using standard form contracts. Sixth, companies should be aware of various scenarios that would require parental consent for children under the age of 13, as specified in COPPA. Finally, it is preferable to require users to certify their continued assent to terms of service on a periodic basis. This will make it far easier for companies to enforce amendments to their terms of service, as some courts have found that terms provided to a user after initial contract formation are unenforceable. *Schnabel v Trilegiant Corp.*

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 Electronic Signatures in Global and National Commerce Act of 2000 (the ESIGN Act) is the primary law regarding the enforceability of contracts formed over the internet. The ESIGN Act provides that contracts may be formed via electronic means and that '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'. Section 103 provides that its provisions do not apply to: (i) wills, codicils and testamentary trusts; (ii) laws governing domestic law matters; (iii) state Uniform Commercial Codes, except section 1-107 and section 1-206, article 2, and article 2A; (iv) court orders and notices; (v) utility cancellation notices; (vi) default, foreclosure or eviction notices; (vii) health or life insurance benefit cancellation notices; (viii) product recall notices; and (ix) hazardous, toxic, or dangerous materials notices. The ESIGN Act does not distinguish between business-to-consumer and business-to-business contracts, though courts may be more sceptical of electronic business-to-consumer contracts absent express evidence of assent on the part of a consumer.

The Uniform Electronic Transactions Act (UETA) is a state-based analogue to the ESIGN Act that has been passed by 47 states, the District of Columbia, Puerto Rico and the US Virgin Islands. Unlike the ESIGN Act, the UETA only applies to business, commercial (including consumer) and governmental matters. Like the ESIGN Act, the UETA provides that contracts may be formed electronically and evidenced by electronic signatures. While the provisions of the ESIGN Act and the UETA are largely the same, the ESIGN would trump the UETA in the event of any conflict between their respective provisions. Regardless, in the context of specific commercial transactions it is advisable to determine whether and to what extent state law may affect a given contract.

In addition, the UCC provisions regarding contracts were not supplanted by the ESIGN Act or the UETA, and continue to affect all contracts related to the sale or leasing of goods in all jurisdictions other than Louisiana, which has not adopted article 2 of the UCC. These provisions apply to both business-to-business and business-to-consumer transactions. However, the precise language of these provisions will vary from state to state, so practitioners should carefully consider the effect of state law on specific commercial transactions over the internet.

The Uniform Computer Information Transaction Act (UCITA) was a proposed uniform state law that would provide significant protections to software makers by permitting them to use shrink-wrap agreements to limit their liability for product defects and to transfer software via a licence to eliminate the ability to resell software under the first sale doctrine of US copyright law. However, the UCITA was only passed in two states, Virginia and Maryland, and numerous states (including Iowa, North Carolina, West Virginia, Vermont and Idaho) have passed so-called 'bomb-shelter' laws expressly protecting consumers from UCITA provisions. These laws specifically permit courts to disregard choice of law or choice of venue clauses in software licences permitted by the UCITA. Consequently, in 2003 the American Bar Association withdrew its approval recommendation of the UCITA as a uniform law provision. Thus, while the UCITA may have had impact in Maryland and Virginia, its provisions have been rejected (or affirmatively thwarted) by a number of state governments, indicating a critical lack of consensus necessary for uniformity.

The UN Convention on Contracts for the International Sale of Goods, although not US law, applies to e-commerce and international sales of goods.

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

The ESIGN Act defines an '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 ESIGN Act also expressly prohibits any law denying the 'legal effect, validity, or enforceability' of a contract 'solely because it is in electronic form'. In addition, the UETA provides similar provisions regarding the definition and enforceability of electronic signatures. However, the ESIGN Act applies to any contracts involving interstate or foreign commerce. Thus, electronic signatures are recognised as fully valid and enforceable across the United States in virtually all contracts, even in states that have not passed the UETA.

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

The ESIGN Act provides that if any federal law or regulation requires that a document (or particular information) be retained by an individual or company, it may maintain such records electronically so long as they accurately reflect the information set forth in the record, and remain accessible in a form that can be accurately reproduced for later reference. The UETA contains an identical provision. In addition, the ESIGN Act requires that companies provide consumers with information regarding their right to receive paper records, their ability to withdraw consent to receive electronic records, and the hardware and software requirements to access and retain electronic records. Finally, as noted above, it is vital that a business maintains records regarding the precise circumstances regarding any express or implied consent it received related to click wrap or browse wrap agreements to ensure they are enforceable in court, though there is no express provision of the ESIGN Act or UETA requiring them to do so.

Security

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

In the wake of numerous recent high-profile data security breaches, cybersecurity has become a critical issue for companies, with some going as far as appointing a Chief Information Security Officer who has direct responsibility for information security issues. In the US, there is no overarching cybersecurity law. Instead, in addition to state laws and federal agency regulations, HIPAA, GLB, COPPA and the Homeland Security Act provide industry-specific mandates with respect to data security in relation to healthcare organisations, financial institutions, children and federal agencies, respectively. Notably these laws do not provide specificity with respect to the implementation of information security measures and primarily mandate general requirements to implement information security principles. For example, the Federal Information Security Management Act (FISMA), which applies to every government agency, 'requires the development and implementation of mandatory policies, principles, standards, and guidelines on information security.' As another example, COPPA requires online service providers that operate websites directed at children to maintain reasonable procedures to protect the security and integrity of the information collected.

As to state law, most states have implemented data protection laws which set out, among other things, processes for notification of consumers in the event of a data breach, as further discussed below. Many states modelled their legislation after the approach taken in California, but there are variations in state laws as to the nature of the breach that triggers a notification requirement. There are also differences in applicable penalties, so it is important to scrutinise applicable state law requirements in the event of a breach.

The Payment Card Industry Data Security Standard (PCI DSS), which was formed by Visa, MasterCard, American Express, Discover, and JCB, is a uniform information security standard for organisations that handle credit cards. The PCI DSS is administered by the Payment Card Industry Security Standards Council. The PCI DSS requires, among other things, the encryption of transmission of cardholder data across open, public networks.

While HIPAA requires healthcare organisations to implement a mechanism to encrypt and decrypt electronic protected health information, not all applicable federal laws mandate data encryption. However, given the broad requirements to ensure data security under certain federal laws (eg, GLB), in some cases it is best practice to encrypt data both at rest and in transit. The issue of encryption of data at rest and in transit is becoming increasingly important for organisations concerned about cybersecurity risk, and many organisations voluntarily implement measures to encrypt data at all points in the data lifecycle.

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?

There is currently no law with respect to mandatory key disclosure in the US and this issue is currently the subject of intense debate, both among the public and before the courts. However, there are a few cases that provide some guidance. In *In re Boucher*, the court ordered an individual to produce the password to the individual's hard drive to access evidence the government already knew was there. In another recent case, following the terrorist attack in San Bernardino, California in December 2015, a federal judge ordered Apple, Inc to write special software that would help the US Department of Justice (DOJ) circumvent security features on an iPhone used by one of the terrorists. In early 2016, Apple refused and indicated that it would never work with any government agency to create a 'backdoor' in any of its products or services. The Federal Bureau of Investigation (FBI) ultimately paid a third party to unlock the phone. In a further highly publicised case, the operator of the Lavabit secure email service (used by Edward Snowden) was asked to produce a private SSL encryption key. The owner of Lavabit was held in contempt of court and shut down his company but the court never ruled on the substantive legal issue of whether the government had the authority to compel Lavabit to produce its encryption keys. One recent issue that has arisen in this area is the extent to which the Fifth Amendment (ie, privilege against self-incrimination) limits the ability of law enforcement to force a suspect to enter his or her password to decrypt a computer. In *United States v Apple MacPro Computer*, the Third Circuit held that, 'where the production of evidence would concede the existence, custody, and authenticity of that evidence, the Fifth Amendment privilege against self-incrimination would apply' and a suspect would not be required to decrypt a device. However, the Fifth Amendment would not protect an act of production 'when any potentially testimonial component of the act of production' (eg, the existence, custody and authentiticity of the evidence) is a 'foregone conclusion' that adds little or nothing to the sum total of the government's information'. Further, in order for an individual to be compelled decrypt his or her device without falling foul of the Fifth Amendment, law enforcement must be able to 'describe with reasonable particularity' the documents or evidence it seeks to compel. A report published in July 2015 by MIT Computer Science and Artificial Intelligence Laboratory explains the security issues that arise from making a key available to a third party to decrypt information. Ultimately, the report suggests that if law enforcement prioritises exceptional access, then it needs to provide evidence and develop detailed specifications for what the exceptional access mechanisms are expected to do.

In light of the foregoing, several bills have been introduced in Congress and at the state level that aim to ensure that law enforcement bodies have a means of accessing the contents of encrypted devices (eg, by requiring companies to build 'back doors' into their devices that would allow the government to obtain encrypted information on such devices in the event that the government obtains a warrant to do so). At the same time, hardware and software companies continue to design and build devices and operating systems that contain increasingly stronger encryption methods. Some companies (eg, Apple, Google) are even going so far as to eliminate their ability to unlock or otherwise extract data from their encrypted devices.

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 registered by certain accredited bodies called domain name registrars. A domain name registrar is accredited by an entity called the top level domain (TLD) registry. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for, among other things, bestowing accreditation on non-country specific TLD registrars (eg, .com, .net, etc). Since 2011, there are fewer restrictions on becoming a registrar for non-country specific TLDs and a new generic top-level domains programme has been established by ICANN. ICANN and other TLD registries have the power to de-accredit domain name registrars that are in violation of their policies and procedures. The Registrar Accreditation Agreement, 2013 provides increased security and protection for domain name registrants.

There are specific criteria that must be met for registration of a '.us' domain name, which criteria are based on the registrant having a sufficient US nexus and bona fide presence in the US. One of the following territorial requirements must be satisfied in order to demonstrate a sufficient US nexus: (i) if the registrant is a natural person, the registrant must be a US citizen, a US permanent resident or have its primary domicile in the US; or (ii) if the registrant is an entity or organisation, the registrant must either be incorporated in the US or have a bona fide presence in the US.

12 Do domain names confer any additional rights beyond the rights that naturally vest in the domain name?

A domain name is frequently used to identify the source of information and therefore is used, in effect, as a trademark. The domain name owner can thus develop common law rights in a domain name, which may become capable of registered trademark protection. However, the nature of rights in domain names has not, to date, been adequately addressed by courts, and so remains an open legal question.

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

An arbitration proceeding may be filed against an erroneous or improper registration of a domain name under the Uniform Domain Name Dispute Resolution Policy (UDRP). A lawsuit may also be filed under the Anti-Cybersquatting Consumer Protection Act of 1999 (ACPA) for abusive use of domain names. The owner of a trademark can use evidence of ownership to show that (i) a domain is identical or confusingly similar to his, her or its trademark; (ii) the domain name was registered in bad faith; and (iii) the domain name registrant lacks legitimate rights in the domain. The UDRP and ACPA provide for other factors by which a complainant may show bad faith on the part of a domain name registrant. In the event of a violation under ACPA, relief may be awarded by way of cancellation of the domains or monetary damages (among other remedies).

Advertising

14 What rules govern advertising on the internet?

Online advertising is subject to the same general laws and regulations (and self-regulatory codes) as conventional advertising. For example, the FTCA authorises the FTC to prevent deceptive and unfair actions that affect competition and commerce. This includes truth-in-advertising regulations related to the sales of products and services, which prohibit a company from engaging in representations, omissions or practices that are likely to mislead or improperly influence consumers. Similarly, there is a wealth of both state and federal law governing both conventional and online advertising, both via

government action and civil claims from competitors, consumers, and even putative classes. Accordingly, an organisation should employ the same stringent controls for online advertising as it would do for conventional forms of advertising.

In recent years, numerous laws intended to regulate direct marketing to consumers (eg, the CAN-SPAM Act of 2003 and the Telephone Consumer Protection Act of 1991 (TCPA)) have been vehicles both for government enforcement actions as well as massive civil class action lawsuits. As such, it is vital for companies to understand and comply with their obligations under these acts.

The CAN-SPAM Act imposes several restrictions on any senders of commercial email messages:

- each email must contain a visible and operable opt-out mechanism;
- all opt-out requests must be honoured within 10 days, and opt-out lists can only be used for compliance purposes;
- each email must include accurate 'From' lines and relevant, non-deceptive subject lines;
- each email must list a legitimate physical address of the publisher or advertiser;
- any emails containing adult content must contain a label to that effect; and
- each email must identify that it is an advertisement absent 'affirmative consent' by the recipient of the email.

In some cases, companies can be found liable for criminal violations of the CAN-SPAM Act if they engage in certain fraudulent conduct such as sending emails through hijacked computers, using false internet protocol addresses, disguising the source of emails, using falsified information in the header, or using email accounts gathered via falsified account registration information. Both the FTC and federal law enforcement officials have been involved in numerous efforts to enforce the CAN-SPAM Act via criminal and civil proceedings. While several states have enacted similar state laws, some federal courts have found that the CAN-SPAM Act pre-empts any such legislation, and the statute itself purports to 'supersede any statute, regulation, or rule of a State [...] that expressly regulate[s] the use of electronic mail to send commercial messages' unless it relates to 'falsity or deception in any portion' of such an email.

The CAN-SPAM Act also empowered the FCC to develop additional rules regarding the sending of commercial emails and text messages to wireless devices. For commercial emails sent to wireless devices: (i) a recipient must consent to receive such emails in writing; (ii) the sender must identify the name of the entity sending the messages and the entity advertising products and services; and (iii) the sender must provide an opt-out that provides recipients to opt-out the same way they opted-in and honour any opt-out requests within 10 days. For commercial text messages, a recipient must provide express consent in writing (though 'information' texts may be sent upon oral consent). At the time of consent, an advertiser is required to make clear that the subscriber has agreed to receive advertisements to his or her wireless device, that the identity of the advertiser is disclosed, that the subscriber may incur charges for these messages, and that they can revoke consent at any time. The FCC maintains a list of wireless domains to assist companies in determining what emails may be sent to wireless email addresses or devices, and advertisers can seek a limited exemption for domains not included on this list for 30 days prior to the initiation of a given advertisement.

Businesses should also be aware of the potentially devastating impact that violations of the TCPA can have for companies. The TCPA places strict limits on a company's ability to use landline or cell phones, SMS text messages and facsimiles to engage in direct advertising absent a recipient's prior express consent (though in the case of a facsimiles an existing business relationship may permit faxing if FCC-proscribed opt-out language is included). Notably, the TCPA provides for damages of US$500 for each violation. While this might render individual claims fairly easy to remedy, in recent years plaintiffs' attorneys have taken advantage of the TCPA's allowance of private rights of action to pursue class actions, and the vast majority of courts have granted certification absent strong evidence that the claims of the putative class are highly individualised. By contrast, the CAN-SPAM Act's limited private right of action has largely precluded similar suits. Moreover, because the TCPA places no cap on the aggregate damages available and does not limit the ability to pursue claims via class actions, the damages available can be potentially catastrophic. Recent settlements in TCPA cases evidence this fact. In 2016, three cruise marketing companies – Caribbean Cruise Line, Inc, Berkley Group Inc and Vacation Ownership Marketing Tours Inc – agreed to create a common fund of up to US$76 million in connection with a class action settlement regarding illegal robocalls to cell phones and landlines. In 2014, Capital One agreed to a class action settlement of US$75.5 million over claims related to autodialled calls to cell phones. While FCC enforcement in this area has been very limited, the potentially massive civil liability such marketing can generate warrants careful consideration. This is particularly true since computer- or internet-based services are often used both to collect customer contact lists and to generate and transmit calls, texts, and even facsimiles. Many states have enacted similar laws, though in most cases plaintiffs' attorneys primarily focus on their TCPA claims given their high value; there remains an ongoing question as to whether the TCPA may pre-empt some or all of these laws.

COPPA also serves to regulate the conduct of online advertisers as it relates to the collection of personal information for those less than 13 years of age. Prior to the collection such information, companies must post a comprehensive online privacy policy outlining their practices regarding data collection and use, obtain verifiable parental consent, provide reasonable means for parents to review collected information or to refuse the further use or maintenance of the same, and carefully protect such information. Companies are also prohibited from conditioning a child's use of their services on providing more information than is reasonably necessary. In addition, since 2013 the FCC has made clear through the first amended COPPA Rule that COPPA applies both to a website and any outside services (eg, plugins such as a Facebook 'like' button or affiliate advertising networks) that are integrated therein as well as mobile apps. Moreover, mobile apps are prohibited from including behavioural advertising (eg, targeting ads to children based on the use of that app) or 're-targeting' ads based on browsing history without parental consent. While the FTC has brought many enforcement actions asserting COPPA violations, these actions are typically resolved through settlement agreements, pursuant to which a company agrees to pay civil penalties historically ranging from US$300,000 to US$800,000.

Finally, private industry groups such as the National Advertising Division (NAD), the Children's Advertising Review Unit (CARU), the Electronic Retailing Self-Regulation Program (ERSP), the National Advertising Review Board (NARB) and the Online Interest-Based Accountability Program serve as self-regulatory agencies for advertising and conduct investigative, enforcement and appellate proceedings. These organisations also set out guidelines to be followed by advertisers. The NAD in particular is a common vehicle used by private companies to evaluate the truth and accuracy of national advertising, including, by way of example, surveys, product testing and pricing claims. NAD challenges are typically originated by a competitor, though the NAD also monitors national advertising and may initiate proceedings based on consumer or advocacy group complaints. NAD proceedings are conducted according to procedures developed by the organisation (the Advertising Industry's Process of Self-Regulation, Policies and Procedures by the National Advertising Review Council). Advertisers that decline to participate in NAD proceedings will find claims are referred to appropriate regulatory agencies (eg, the FTC or FDA). The NARB is tasked with adjudicating appeals of rulings from the NAD. Both the ERSP and the CARU employ similar procedures respectively for direct advertising via 800 numbers, emails, websites and ads targeting children (including issues of COPPA requirements). Notably, companies that comply with CARU guidelines are deemed to be COPPA-compliant, and are effectively protected from FTC enforcement actions. Thus, these bodies serve a vital function in the context of internet advertising and companies engaging in such advertising should be aware of their policies and enforcement practices.

15 How is online advertising defined? Could online editorial content be caught by the rules governing advertising?

There is no explicit regulation or case law differentiating online advertising from online editorial content. As noted below, even incidental commercial links or functions on a site can convert it from a purely expressive website to a 'commercial use' that could be considered advertising. Some cases related to section 230 of the Communications Decency Act of 1996 (Title V of the Telecommunications Act) have

drawn a distinction between sites that are merely a conduit through which advertisements are conveyed (eg, a newspaper or an online marketplace like Backpage or Craigslist) and the parties that actually generate and benefit from such advertisements (eg, the entity placing the ad). *Jane Doe No. 1 v BackPage.com, LLC*.

In recent years, publishers and marketers started producing content called 'native advertising', which is a form of advertising commercial content masked in an editorial format. Native ads do not outwardly appear as traditional ads (eg, pop up windows and banners): rather, these ads draw on the design, feel, and style of the surrounding media, blending editorial and advertising content, to promote a product or service. For example, marketers have created native ads through news platforms and popular Instagram accounts by sponsoring an article, pos, or product review, hoping to increase the visibility of their brands in a less disruptive manner. Given the tension between attempting to portray organic content on a media platform and featuring a commercial product or service, the FTC released Native Advertising: A Guide for Businesses (the Native Ad Guide) in December 2015 to address the risk of misleading consumers. The Native Ad Guide provides detailed recommendations on how to make clear and prominent disclosures to avoid deceiving consumers. Since there is very little guidance on where the line is drawn between advertising and editorial content, companies should be mindful of the potential implications of their online publishing, particularly as native advertising becomes a common revenue stream for many media platforms.

16 Are there rules against misleading online advertising?

As noted above, online advertisements are subject to the same FTC regulations as conventional advertisements with regard to misleading advertisements. The FTC imposes a 'reasonable basis' standard on business regarding advertising claims. This means that firms must have a reasonable basis to support any claims made in their advertising, and retain records sufficient to establish their basis for that belief if asked to do so. While this standard is consistently applied across all industries, the level of substantiation required will vary based on the specificity and force of the claims made within a given advertisement, as well as whether a claim is explicit or implied. In addition, the FDA maintains its own set of rules and standards for the advertising of foods and drugs, and provides ample guidance online about its standards. These standards may implicate misleading advertising claims, including, for example, so-called 'green claims' describing a product as 'organic' or 'all natural'. Unlike the FTC's reasonable basis standard, these FDA standards are far more specific to given products and industry and thus require careful consideration when analysing advertising claims that could fall within the purview of the FTC. Finally, companies should bear in mind that state and federal law provides methods for plaintiffs (including both competitors and consumers) to bring lawsuits related to false or misleading advertising. Thus, it is important for companies to carefully substantiate advertising claims and to maintain records sufficient to support that substantiation in the event of future enforcement or civil actions.

17 Are there any products or services that may not be advertised on the internet?

The US does not have any regulations proscribing the advertising of specific goods and services online. Companies should obviously be careful not to actively advertise illegal goods and services unless they are acting solely as an interactive computer service for the purposes of section 230 and users are placing such advertisements. Some critics claim that section 230 grants overly broad protection to online content providers, as such providers are granted broad immunity against liability for the content posted by others. For example, in various cases from 2010 to 2017, courts have protected Backpage.com LLC, a classified advertising website, from claims that it allegedly enabled sex traffickers to advertise their victims online. Further, as noted below, case law suggests that companies can be found liable if they offer services that are found to discriminate against individuals that are members of a protected class. *Fair Housing Council of San Francisco v Roommates.com, LLC* and *McKinley v eHarmony*. As is also noted below, any advertising related to online gambling can be dangerous given the complex web of state and federal regulations governing its legality in the United States.

18 What is the liability of content providers and parties that merely host the content, such as ISPs? Can any other parties be liable?

As explained in detail in the following section, sites that host content (such as ISPs) are not generally liable for content hosted on their sites pursuant to section 230.

Financial services

19 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?

The advertising and selling of financial services products (both through conventional means and via the internet) is highly regulated in the US. The same consumer protection laws that apply to advertising commercial products and services also apply to the online advertising of financial services products. For example, under the FTCA, advertising (i) must be truthful and non-deceptive; (ii) must be substantiated; and (iii) cannot be unfair. As to laws that are germane to financial services, as one example, under the Truth in Lending Act, advertisements for consumer credit must include certain disclosures about the terms and conditions of the credit offered. In particular, it requires that disclosures are clear and conspicuous to enable consumers to readily understand the information. In 2011, in response to the financial crises, the FTC issued a new rule with respect to deceptive mortgage ads. The rule provides numerous examples of prohibited deceptive claims, including the type of mortgage offered and the existence, nature and amount of fees or costs to the consumer associated with the mortgage. The FTC also has jurisdiction over non-financial services entities that provide services to or on behalf of a bank.

Apart from the FTC, the other key regulatory body with respect to financial services is the SEC, which oversees conduct in the security industry. Under the Securities Act, it is unlawful for any person, in the offer for sale of any security, by the use of any means or instruments of transportation or communication in interstate commerce or by use of mail, to, among other things, employ any device, scheme or artifice to defraud or to engage in any transaction or practice that operates as fraud or deceit on the buyer or both. These rules would apply equally to the sale of securities over the internet. The SEC has also recently adopted detailed measures to regulate the advertising of crowdfunding campaigns.

Notably, states have also increased regulations regarding advertising or selling of financial services or products to consumers or to businesses via the internet, and these must be considered in each state. Additionally, many state insurance departments mandate that insurance advertisers comply with detailed requirements including use of the insurer's full name; identifying additional costs for endorsements or riders and, when a premium is referenced, the specific cost of referenced endorsements or riders; referencing complete and accurate statistics; and specifying the offer of non-contractual benefits.

Defamation

20 Are ISPs liable for content displayed on their sites?

ISPs are generally not liable for materials posted on their sites. Section 230 specifically provides immunity to providers and users of any 'interactive computer service' that publish information provided by third parties: '[n]o provider of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.' The term 'interactive computer service' is defined broadly, and expressly includes any 'service or system that provides access to the Internet'. Section 230 was passed in part as a reaction to the 1995 New York state court decision *Stratton Oakmont, Inc. v Prodigy Services Co.* holding that online service providers could be held liable for the speech of their users because they maintained 'editorial control' over users by posting and enforcing general content guidelines. Thus, section 230 was designed to avoid creating a disincentive for ISPs and other online service providers to monitor user content by limiting their liability for the speech of their users. This immunity is not unlimited, as claims related to federal criminal liability or intellectual property claims are expressly exempted from section 230 immunity (subject to the separate copyright safe harbour provided under the DMCA). Nonetheless, federal courts have usually held that

section 230 provides complete immunity for ISPs regarding torts committed by their users or via their systems, including defamation claims. *Zeran v AOL*.

However, ISPs may find themselves liable in cases where they have a substantive role in the creation or modification of content. In cases where an ISP or internet service 'is responsible, in whole or in part, for the creation of development' of content, they are deemed 'information content providers' and lose section 230 immunity. For example, two websites that offer a forum for customers to submit complaints about businesses ('Rip-off Report' and 'Bad Business Bureau') have been repeatedly found potentially liable for defamation because they have created titles, heading, comments, and editorial messages in connection with content submitted by users. *MCW, Inc. v Badbusinessbureau.com, LLC* and *Whitney Information Network, Inc. v. Xcentric Ventures LLC*. Courts have also found that sites that 'materially contribute' to the unlawful nature of content (eg, by posting questionnaires including mandatory, pre-populated answers) may be considered 'information content providers' for the purposes of section 230 immunity. *Fair Housing Council of San Francisco v Roommates.com, LLC*. Moreover, some courts have held that websites that are aware of potential threats against individuals posted by users of their sites may have a duty to warn such individuals, even if they are not liable for the posting of the threats themselves. *Jane Doe 14 v Internet Brands, Inc*. Thus, while courts typically provide broad immunity to ISPs and websites that post user content, that immunity is not absolute.

Finally, while section 230 immunity may apply to ISPs in the context of defamation cases, that immunity does not extend to their users. Thus, courts may require ISPs to disclose the identity of anonymous users that post allegedly defamatory comments on the internet if the right of the plaintiff to seek redress outweighs the user's First Amendment right to anonymity. *Independent Newspapers Inc. v Brodie* and *SaleHooGroup, Ltd. v ABC Co*. Courts have quashed subpoenas in cases where a plaintiff fails to offer sufficiently specific evidentiary support for each element of their defamation claim, even if their allegations would otherwise be sufficient to withstand a motion to dismiss or a motion for summary judgment.

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

Section 230 does not require ISPs to shut down web pages containing defamatory materials, even in cases where the ISP has been made aware of the allegedly defamatory content. Of course, the purpose of section 230 was to enable ISPs to monitor and edit user content without running the risk that they be found liable as a publisher. Thus, ISPs are free to voluntarily remove defamatory content, or indeed any content they deem inappropriate or offensive (even if otherwise protected under the Constitution). Moreover, this right may be limited to the extent that an ISP or website has separate agreements or terms of service that impose limits on the monitoring or removal of content. In addition, if an ISP or website reneges on a promise to remove third-party content, they may be subject to a promissory estoppel claim. Thus, while section 230 does not limit an ISP's ability to voluntarily remove defamatory content, ISPs should be mindful of potential contractual issues that could impose liability for the removal (or failure to remove) user content.

Intellectual property

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

There is no US legislation that prohibits or limits a website from linking to third-party websites. However, in some cases the terms of service for a website may purport to impose limits on a user's ability to reproduce or link to content from a website directly or indirectly. Moreover, cases like *Kelly v Arriba Soft Corp.* and *Perfect 10, Inc. v Amazon, Inc.* have confirmed that 'deep-linking' (ie, linking directly to specific content on a website rather than a website's homepage) is also permissible in the United States. Nonetheless, as discussed below, businesses should be mindful of potential liability that can arise from linking to third-party websites. As a matter of best practice, businesses can ask creators of original content for permission and subsequently enter into a 'linking agreement' or place clear and prominent linking disclaimers.

23 Can a website owner use third-party content on its website without permission from the third-party content provider? Could the potential consequences be civil in nature as well as criminal or regulatory?

US copyright law provides strict protections for any and all creative works fixed in a tangible medium of expression, including works with only 'minimal' creativity. As such, the use of third-party content on a website without the authorisation of the creator of that content can result in both civil and criminal liability. In some cases, the doctrine of 'fair use' may serve to immunise certain uses of third-party content. Courts consider four factors in determining whether fair use applies: (i) the purpose and character of the use; (ii) the nature of the copyrighted work; (iii) the amount and substantiality of the portion taken; and (iv) the effect of the use upon the potential market. In the online context, one of the key considerations regarding the applicability of fair use is whether a given use is 'transformative' (ie, used for a different purpose than the original content). In addition, fair use is more commonly found where the accused infringer did not appropriate a 'substantial' amount of the original content. Several cases provide guidance about the approach courts have taken to applying fair use to the internet. In *Kelly v Arriba Soft Corp.*, the court held that search engines' use of thumbnails images generated by deep-linking to full size images on a third-party site constituted fair use. Some legal commentators explain that under *Kelly*, website owners may not be able to hold web crawlers or web scrapers liable for copyright infringement. In *Author's Guild, Inc. v Google, Inc.*, the court found that the mass digitisation of books from various research libraries for the purposed of data and text mining also constituted fair use. This ruling was largely re-affirmed in *Authors Guild, Inc. v HathiTrust*, where the court emphasised the benefits such data and text mining provided to academic inquiry. In addition, courts have been supportive of uses that constitute commentary or criticism of the content of others. For example, in *Righhaven v Hoehn*, the court held that posting an entire editorial from a newspaper as part of an online discussion constituted fair use. However, in *BWP Media USA, Inc. v Gossip Cop Media, LLC*, the court found that a gossip website's unauthorised use of photos did not constitute fair use, since the website merely used the photos to report the same narrative as other websites. Additionally, recent Supreme Court precedent strongly suggests that websites and web services cannot allow users to view live or time-shifted streams of over-the-air television via the internet. *American Broadcasting Companies v. Aero*. In sum, a fair-use analysis is necessarily a fact-intensive inquiry, and companies considering the applicability of this defence should carefully analyse the various factors used by courts in determining whether fair use applies to a given use.

The use of third-party content can also result in potential trademark law liability. Though various multi-factor tests are used by courts to determine whether trademark infringement has occurred, liability often arises when one uses another's trademark in commerce without the permission of the owner in a manner that is likely to cause confusion. The difficulty in applying trademark law in the context of the rapidly evolving realm of the internet led one court to claim it 'is somewhat like trying to board a moving bus'. *Bensusan Restaurant Corp. v. King*. Nonetheless, some trends have developed that provide guidance on key issues. Generally speaking, courts have found that the use of another's trademark in a domain name constitutes trademark infringement when used for commerce and likely to confuse consumers. *1-800 Contacts, Inc. v WhenU.com*. However, courts have permitted the use of trademark in the domain name of 'gripe sites' designed to criticise a company. *Ford Motor Co. v 2600 Enterprises* and *Utah Lighthouse Ministry v Found. for Apologetic Info. & Research*. Similarly, social media platforms have allowed users to create accounts that incorporate another person's or entity's registered trademark since such platforms are primarily expressive in nature – though many of those platforms, including Facebook, Twitter and Instagram, have implemented a 'verified' feature that authenticates the actual user or trademark owner. When a trademark is used on a site in manner that markets competing goods or directs consumers to sites where they can make purchases from competitors, such use may constitute infringement. *1-800 Contacts, Inc. v Lens.com*. By contrast, a court has found that the use of trademarks in headlines and banner ads constituted permissible 'nominal use,' though the use of the same trademarks in site wallpaper does not. *Playboy Enterprises, Inc. v Welles*. Courts have similarly held that the use of 'framing' (ie, allowing users to visit another site in a 'frame'

without leaving the original site) may constitute trademark infringement or dilution (*Digital Equipment Corp. v AltaVista Technology*), but that linking to another website does not (*Ticketmaster Corp. v Tickets.com, Inc.*). However, recent case law strongly suggests that 'framing' would be treated the same as linking in the future. *Perfect 10, Inc. v Google, Inc.*

Generally speaking, the use of third-party trademarks in 'metatag' keywords constitutes a 'use in commerce' that can result in a claim for trademark infringement. *Rescuecom Corp. v Google, Inc*. Courts have recently held that a search engine is not itself liable for selling a trademarked name to a competitor via its online advertising platform. *Rosetta Stone Ltd. v Google, Inc*. Nonetheless, many commentators now believe that the trends suggest that keyword advertising programs like 'AdWords' are likely protected from trademark infringement claims. *CollegeSource, Inc. v AcadmyOne, Inc.* and *General Steel Domestic Sales, LLC v Chumley*. Regardless, liability may still arise where a purchased keyword is used in connection with an ad or website link that may result in source confusion. *CJ Products, LLC v Snuggly Plushez LLC*. Notably, the doctrine of fair use, described above, also applies in the context of trademark infringement, and some cases have found the use of trademarks in metatags may constitute a fair use in the context of 'gripe sites' or where the use is nominal. *Bihari v Gross* and *Playboy Enterprises, Inc. v Welles*.

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

A website owner can exploit the software used for a website by licensing it to third parties so long as it is the owner of, or has sufficient rights in, any intellectual property rights associated with that software. Software can encompass both patent law (eg, the concept of the software) and copyright law (eg, the underlying source code). If a website owner licensed or purchased software from a third party to build its site, it cannot license or sell that software to other third parties absent an express grant of authority by the creator of the software.

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

As discussed above, linking to third-party websites is permissible, though in some cases it can result in liability for trademark or copyright infringement. The 'safe harbour' provision of the DMCA protects online service providers that act as a 'data conduit' (including ISPs) from liability copyright infringement resulting from linking to, or hosting, infringing content. In order for this safe harbour to apply, an online service provider must:

- have no knowledge of, or financial benefit from, infringing activity on its network;
- once provided with knowledge, act expeditiously to remove or disable access to the infringement materials;
- have a copyright policy and provide proper notification of that policy to its subscribers; and
- list an agent to deal with copyright complaints.

Users of a site are permitted to file a counter-notice in response to a DMCA takedown request claiming that the materials do not infringe the complainant's copyrights. If the copyright owner does not notify the online service provider within 14 days that it has a claim against the user in court, these materials can be restored. This 'safe harbour' has been held repeatedly to protect numerous websites, including video content providers like YouTube and Vimeo. *Viacom Intern., Inc. v Youtube, Inc.*, *IO Group v Veoh Networks, Inc.* and *Capitol Records, LLC v Vimeo, LLC*. However, sites can be liable under the DMCA for hosting or linking to software or devices intended to circumvent digital rights management associated with copyrighted materials. *Universal City Studios, Inc. v Reimerdes*. Moreover, the Ninth Circuit recently noted that online moderators, who can approve or remove user-uploaded content, may not fall within the DMCA safe harbour depending on the extent of the moderator's involvement in screening and posting. *Mavrix Photographs, LLC v LiveJournal, Inc*.

As discussed above, linking to third-party websites can also result in liability for trademark infringement provided that the link is used in connection with the sale of goods and services. Hyperlinking and deep-linking will not constitute trademark infringement unless they generate source confusion. *Ticketmaster Corp. v Tickets.com*. Similarly, 'gripe sites' are permitted to link to a trademark owner's website. *Knight-McConnell v Cummins*. However, when a website offers links to commercial goods and services, it may serve to convert otherwise permissible uses to infringing commercial uses. *PETA v Doughney* and *Taubman Co. v Webfeats*. However, case law in this area is mixed, as some cases have found that a site may link to its own online store selling products without converting an expressive web page into a commercial one. *Utah Lighthouse Ministry v. Foundation for Apologetic Information and Research*. Similarly, merely linking to another site that includes advertisements will not convert an expressive website into a commercial one. *Boseley Medical Institute, Inc. v Kremer.*

26 Is video content online regulated in the same way as TV content or is there a separate regime?

TV content is generally subject to more stringent content regulation than online video content. In *Reno v ACLU*, the Supreme Court struck down anti-indecency provisions in the Communications Decency Act that would apply to 'obscene or indecent' material on the internet as violative of the first amendment. By contrast, the FCC is permitted under federal law to regulate the airing of obscene material via radio stations and over-the-air television states at any time and the airing of 'indecent' material between 6am and 10pm. However, this standard only focuses on 'material that describes or depicts sexual or excretory material', and not on the use of smoking, drugs or violence. However, as noted above, copyright and trademark laws apply in equal force to both online and TV content, as well as the advertising regulations referenced above and other various state and federal laws. Nonetheless, even a casual observer of the internet will be able to quickly discern that the sheer volume of online content creates a 'wild west' atmosphere where boundaries are often tested and enforcement actions are difficult to identify and prosecute.

27 Do authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

The FBI is actively involved in investigating and prosecuting intellectual property theft in the context of copyright law and trade secrets, though wilful trademark infringement can also give rise to potential criminal liability (though only in the case of counterfeit goods). At present, there are no criminal penalties associated with patent infringement. According to section 502 of the Copyright Act, federal criminal penalties for copyright infringement are only triggered where an infringer acts 'for the purpose of commercial advantage or private financial gain'. Federal authorities can and do pursue seizures related to copyright infringement, including websites as well as infringing goods, though traditional injunctive relief is not available in criminal copyright infringement cases. For example, in 2012 the FBI, DOJ and the National Intellectual Property Rights Coordination Center (NIPRCC) seized the website Megaupload after an indictment alleging it was illegally harbouring millions of copyrighted files. The FBI is also authorised to destroy any infringing goods it seizes. It is also common for the FBI to seize and destroy counterfeited goods (and even websites selling counterfeit goods) in connection with criminal investigations.

In addition, the Economic Espionage Act criminalises the theft of trade secrets and other forms of industrial espionage, which are a form of intellectual property, and provides the ability to seize appropriate materials before a trial and to enjoin further violations of the act. Moreover, the Defend Trade Secrets Act, signed into law in May 2016, provides an ex parte seizure procedure to use in extraordinary circumstances where the party who allegedly misappropriated a trade secret 'would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person...'. In general, injunctions against copyright, trademark, and patent infringement are primarily provided via civil lawsuits rather than criminal ones. In the United States, it is more common for IP owners to prosecute their rights via the civil system, particularly in the context of trademark law, because of the wide range of remedies available for intellectual property owners and the limited resources of the FBI to investigate the theft of IP. In addition, federal customs authorities are often involved in the enforcement of exclusion orders by the ITC and are able to stop the importation of goods the ITC has found to infringe a third-party's IP rights.

28 What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

IP owners in the United States are provided with a wide range of remedies in civil litigation that can include search orders and injunctive relief. Under the Copyright Act, a copyright owner in a civil case can seek both preliminary and permanent injunctions against copyright infringement, as well as the impounding and destruction of infringing materials via a seizure order. The Lanham Act also permits a trademark owner in a civil case to seek both preliminary and permanent injunctions against trademark infringement as well as the seizure and destruction of infringing labels, signs, prints, packages, wrappers, receptacles and advertisements found to infringe. Similarly, upon a finding of infringement patent owners are entitled to both preliminary and permanent injunctions preventing ongoing patent infringement (eg, manufacturing or selling an infringing product) and courts may order the recall, seizure and destruction of infringing goods. *Nike, Inc. v QiLoo Intern. Ltd*.

Data protection and privacy

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

In the US, there is no single law with respect to data privacy; instead there is a patchwork of federal and state laws and industry standards that regulate the collection, use, processing, disclosure and security of personally identifiable information (PII). It is worth noting that these laws and regulations often overlap, and at times may contradict one another. It is also worth noting that may federal privacy laws apply only to specific business sectors or categories of information (eg, financial institutions (in the case of GLB) and health information (in the case of HIPAA)). In addition to these laws and regulations, there are many guidelines that have been developed by governmental agencies and industry groups that may not be legally enforceable but can be used as a guide to 'best practices' with respect to the collection, use, processing, disclosure and security of PII.

Many states define PII as an individual's last name in combination with another data point, such as a social security number. The National Institute of Standards and Technology Special Publication 800-122 defines PII as 'any information about an individual maintained by an agency, including (i) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.' In effect, if there are two data points, such as part of a name and an address that could be connected to identify an individual, such information may be considered PII. However, definitions may vary and it is important to carefully consider the definition applicable under a particular state law or industry standard.

30 Do parties involved in the processing of personal data, such as website owners, have to register with any regulator to process personal data?

Under US law, there is no obligation for website owners to register with a regulatory body to process personal data, nor is there a requirement that parties involved in processing personal data appoint an in-house data protection officer. However, most states have some form of data breach notification requirement, so website owners would have obligations to notify regulators in the event of a data breach.

31 Could data protection laws and regulatory powers apply to organisations or individuals resident outside of the jurisdiction?

While most federal and state data protection laws and regulations on their face apply to organisations and individuals outside the US (eg, the FTCA and all of the other rules and regulations promulgated under the FTC's authority apply to any company or individual doing business in the US), the reach of these laws is generally limited to organisations and individuals that are subject to the jurisdiction of the US (as discussed above).

Under the current European Data Protection Directive 95/46/EC (the Directive), if an organisation has an office, agency or branch in the European Economic Area (EEA), or operates equipment within the EEA (ie, servers), then the Directive will apply to that organisation. Under the Directive, personal data can only be transferred to a jurisdiction that is deemed to provide an adequate level of protection for personal data. Prior to October 2015, the FCC's Safe Harbor programme was approved as a method of providing an adequate level of protection for data transfers to the US. However, on 6 October 2015, the Court of Justice of the European Union invalidated the Safe Harbor framework. However, in July 2016, the EU formally adopted the so-called 'US-EU Privacy Shield', which sets forth the policies and procedures that must be followed in order to ensure an adequate level of protection for personal data for transfers of personal data from the EEA to the US.

However, the General Data Protection Regulation (GDPR), which is due to replace the Directive in 2018, extends the reach of European data protection law to companies that operate websites that are directed at individuals in the EEA or that monitor their behaviour. The GDPR also limits transfers of data outside the EEA to countries that are deemed to provide an adequate level of protection. Notably, the sanctions for non-compliance under the GDPR are substantial: up to 4 per cent of annual worldwide turnover or €20 million, whichever is higher.

Additionally, maintaining a server in a particular jurisdiction may affect an analysis with respect to personal jurisdiction (as discussed above).

32 Is personal data processed on the basis of customer consent or other grounds? What is the commonly adopted mechanism for obtaining customer consent or establishing the other grounds for processing?

The FTCA does not address consent, and does not expressly require a website operator to have or disclose a privacy policy. However, where a website privacy policy has been revised, consumers have to opt-in before the operator can use the PII in a way that is materially different from the privacy policy that was in effect when the PII was collected. In addition, the FTC's Behavioral Advertising Principles recommend that website operators obtain express consent from consumers in advance of collecting sensitive consumer data in connection with online behavioural advertising.

With certain limited exceptions, under COPPA, website operators must obtain verifiable parental consent before collecting PII online from children under the age of 13. HIPAA (also with certain limited exceptions) requires covered entities to obtain written consent from data subjects prior to disclosing such subjects' data. Other laws and regulations (eg, GLB), while not requiring consent prior to processing data, require covered entities to notify individuals of their privacy practices.

At the state level, laws have been enacted in certain states that require consent in certain circumstances. For example, California's medical privacy law (Cal. Civ. Code section 1798.91) prohibits using personal medical information for direct marketing purposes without consent.

33 May a party involved in the processing of personal data, such as a website provider, sell personal data to third parties, such as personal data about website users?

The FTCA does not address sharing information with third parties. However, the FTC takes the view that if an organisation posts a privacy policy that includes a term that the organisation will not sell PII, the organisation must comply with that term.

Other federal laws limit the circumstances under which an entity may disclose PII to third parties. For example, GLB requires that, prior to sharing PII with non-affiliated third parties, financial institutions must notify consumers of their practices with respect to sharing information with third parties, and must grant consumers the right to opt-out if they do not want their PII to be shared. The sharing of personal health information is governed by the HIPAA 'Privacy Rule,' which sets forth the circumstances under which covered entities may share personal health information with third parties. Under HIPAA, there are criminal penalties of up to US$250,000 and imprisonment for 10 years if a violation is committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm.

At the state level, laws related to the sharing of PII with third parties have been enacted in certain states that extend to specific industries or types of data. For example, California's financial privacy law (Cal. Fin. Code section 4050–4060) prohibits sharing or selling personally identifiable non-public financial information without consent. Additionally, under recent California law (Assembly Bill 1710), businesses that

maintain personal information are prohibited from selling, advertising for sale, or offering to sell an individual's social security number.

With respect to students, under the terms of a proposed federal privacy bill, website operators and online service providers would be prohibited from selling students' personal information to third parties and using or disclosing students' personal information to tailor advertising to them. Under California's recent student privacy law (Cal. Bus. and Prof. Code section 22584) website operators and online service providers are prohibited from, among other things, knowingly engaging in targeted advertising to students or their parents or legal guardians or selling a student's information.

34 If a website owner is intending to profile its customer base to carry out targeted advertising on its website or other websites visited by its customers, is this regulated in your jurisdiction?

The FTC's Behavioral Advertising Principles (which are voluntary) suggest that website operators disclose their data collection practices tied to online behavioural advertising that rely on the use of cookies. Otherwise, behavioural advertising is largely self-regulated and several industry bodies, including the BBB have published codes applicable to behavioural advertising.

As set out above, under the terms of a proposed federal privacy bill, website operators and online service providers would be prohibited from selling students' personal information to third parties and using or disclosing students' personal information to tailor advertising to them.

35 Does your jurisdiction have data breach notification or other cybersecurity laws specific to e-commerce?

As noted above, in the US, there is no single law with respect to data privacy; instead there is a patchwork of federal and state laws and industry standards which regulate the collection, use, processing, disclosure and security of PII that are not specifically applicable to e-commerce. In addition, all entities that collect PII may be party to contracts with data subjects that impose breach notification requirements on such entities.

Most states (and the District of Columbia, Guam, Puerto Rico and the US Virgin Islands) have in place data breach notification laws. These laws generally require businesses to take certain steps when a data breach involving PII occurs. For the most part, these laws require notification of the breach to the affected individuals, law enforcement, state regulators, the media and consumer reporting agencies. The laws are typically triggered when the security or confidentiality of PII has been compromised by unauthorised access to data or unauthorised acquisition of data (or both). Most states have a risk of harm threshold before the notification requirements are triggered. While most of the early state security breach laws tended to be reactive in nature (ie, established requirements for responding to security breaches), there has been a recent trend in some states to establish laws that are more preventative in nature (ie, prescribing requirements to avoid security breaches).

While there is currently no overarching federal law that imposes security and breach notification requirements on all entities that collect PII, certain federal laws impose such requirements on certain industries or certain types of data. HIPAA, for example, requires that covered entities notify both the Department of Health and Human Services and each individual whose information has been, or is reasonably believed by the covered entity to have been, improperly accessed, acquired or disclosed as a result of a data breach (subject to certain exceptions). HIPPA also prescribes the content required to be set out in a breach notification, as well as the timing and manner of notification. Similarly, FTC guidelines under GLB require data breach notification when there has been unauthorised access to sensitive customer information, which includes a customer's name, address or telephone number, combined with another identifying data element (eg, social security number, driver's licence number, account number, credit or debit card number, or personal identification number or password that would permit access to the customer's account). Similarly, the FCC has a data breach notification rule, applicable to telecommunications carriers, which includes a requirement for telecommunications carriers to notify federal law enforcement and affected individuals in the event of the intentional and unauthorised access to, use or disclosure of customer proprietary network information (CPNI).

While breach notification requirements are currently limited under federal law, in response to several high-profile data breaches in recent years, several bills have been introduced in Congress that would impose breach notification requirements on all entities that collect PII, regardless of industry.

36 Does your jurisdiction recognise or regulate the 'right to be forgotten'?

The US does not have a 'right to be forgotten'. However, under the California Business and Professions Code, service providers are required to allow children under the age of 18 to remove content that has been posted on a website, online service, online application or mobile application. However, this right is limited to content posted by the person requesting removal of such content. In addition, in February 2017, the New York State Assembly introduced Bill No. A05323, which would require service providers (and any other persons or entities that make information about an individual available on or through the internet) to remove such information upon the request of the individual within 30 days of such request. However, the proposed bill is limited to information that is 'inaccurate, irrelevant, inadequate or excessive' (ie, 'content which, after a significant lapse in time from its initial publication, is no longer material to current public debate or discourse'). Any service provider that fails to comply with such a request will be subject to a fine in an amount that is the greater of: (i) the actual monetary loss for each such violation; and (ii) US$250 for each day of the violation after the removal request, as well as costs for attorneys' fees of the individual requesting removal.

37 What regulations and guidance are there for email and other distance marketing?

There are numerous federal regulations with respect to email and other distance marketing. Current rules and regulations address communications by telephone, fax, mail, email and text message.

Direct mail advertising must comply with the FTCA. The FTCA prohibits unfair or deceptive advertising in any medium, including direct mail advertising.

The TCPA restricts the use of automated telephone equipment (auto diallers) and requires prior express written consent for, among other things: (i) all telephone calls and text messages that use an automatic telephone dialling system or a pre-recorded voice to deliver a telemarketing message to wireless numbers; and (ii) pre-recorded telemarketing calls to residential lines. The TCPA also prohibits sending (i) commercial advertisements to a person or business by fax; and (ii) auto-dialled texts to wireless numbers (unless the caller receives the prior written consent of receiver).

Similarly, the Telemarketing Sales Rules require telemarketers to make specific disclosures of material information, prohibit deceptive telemarketing, set limits on the times telemarketers may call consumers, and prohibit calls to a consumer who have asked to be added to the 'Do Not Call' registry. There is also a Telemarketing Consumer Fraud and Abuse Prevention Act, which prohibits deceptive telemarketing acts.

The CAN-SPAM Act governs unsolicited commercial email communications and prohibits false or misleading email header information and deceptive subject lines, in addition to requiring certain information to be disclosed in email communications and requiring senders to provide recipients with a way to opt out of receiving future email communications. 'Commercial email' is broadly defined under CAN-SPAM as 'any electronic message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an internet website operated for a commercial purpose).' As a result of a recent increase in penalties for violations of CAN-SPAM, violations can be quite costly, as each email sent in violation of CAN-SPAM is now subject to penalties of up to US$40,654 (up from $16,000 per violation). The FTC frequently brings actions against organisations that fail to comply with the CAN-SPAM Act. As one example, the FTC fined Cleverlink Trading Limited US$400,000 for sending emails with misleading headers and deceptive subject lines and without an opt-out mechanism or valid physical postal address (*FTC v Cleverlink Trading Ltd*). As another example, in 2016, the FTC settled a claim against Sale Slash, LLC and other defendants regarding the marketing of certain weight loss pills. As part of the settlement, Sale Slash was required to pay US$43 million in damages (US$10 million of which was paid) and was barred from (i) sending emails that fail to identify the sender, that include misleading subject headings, or that lack a proper opt-out option for recipients; (ii) using fake celebrity endorsements; and (iii)

making weight loss or related claims unless Sale Slash is able to substantiate such claims with scientific evidence.

38 What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Various state laws required that individuals be notified in the event of a data breach. In addition, as noted above, certain federal laws (eg, HIPAA) and regulations require that individuals be notified in the event of a data breach.

Certain state and federal laws allow individuals to sue for privacy violations and these can result in significant damages awards. In 2013, one of the largest data breaches ever at Target stores involved the potential disclosure of payment card information of over 40 million consumers and the personal information of an additional 70 million consumers. Target was sued in class action lawsuits and by shareholders (in addition to being investigated by Congress and state Attorneys General). Similarly, as a result of a massive data breach in 2014, Home Depot, Inc was required to pay US$19.5 million in damages to consumers for losses suffered as a result of the breach, as well as US$25 million to financial institutions.

Taxation

39 Is the sale of online products subject to taxation?

The states of Alaska, Delaware, Montana, New Hampshire and Oregon do not impose a tax on sale of online products. In other states, a tax may apply in the event that there is a taxable nexus between the seller and buyer's jurisdiction, which can be triggered by a contractual obligation or physical presence of seller in the buyer's jurisdiction (eg, a storefront or a distribution centre) or by other business activities conducted in the buyer's location. Some states have adopted the 'click-through nexus approach', which allows tax to be imposed if there is an affiliate in-state resident who refers business to the online seller for consideration. There are also states (eg, Massachusetts) that charge a 'use-tax', which requires persons resident in sales tax states that purchase tax-free items online to pay sales tax directly to their sales tax agency. In the event that an online sale results in a capital gain or business income, such sale may be required to be reported to the Internal Revenue Service for federal income tax purposes. The Housing and Economic Recovery Act of 2008 requires that credit card processing companies report the gross amounts of their merchants' payment card transactions to the Internal Revenue Service. In June 2017, a bipartisan group of Senators reintroduced discussions regarding the Marketplace Fairness Act, a bill that would require state governments to collect sales taxes and use taxes from out-of-state retailers with no physical presence in their respective states.

40 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?

Generally, establishing a server in a state outside the home jurisdiction will be sufficient to trigger the taxable nexus requirement discussed above under question 39 for imposition of sales tax in the state where the server is located. Some states such as Vermont have codified exceptions in their statues which do not consider the presence of a server to be sufficient for taxable nexus. Other states like Washington and California do not tax entities that host services or engage in e-commerce provided on servers located in the state provided these entities do not own the server. States are similarly divided on approach with regard to software as a service (SaaS); for example, the Missouri Department of Revenue ruled that the sale of software hosted on servers located outside the home jurisdiction is not subject to sales tax when accessed from inside the state. In contrast, in New York software services hosted on out-of-state servers are subject to tax in New York if the related software is accessed from within New York.

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

The US does not impose VAT. Sales tax is imposed by states on e-commerce as discussed above under question 39 where there is taxable nexus.

42 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?

This would depend on the facts and circumstances of the sale and applicable state laws, which may vary. Please contact a tax specialist. If the transfer price in connection to the goods returned to the onshore company is unreasonably higher than the costs paid by customer to the offshore seller while purchasing the products online, transfer pricing issues may arise since this could be viewed as an attempt to cut a smaller sales tax deduction from the original online sale.

Gambling

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

Gambling laws in the United States vary from state to state so careful attention must be paid to the laws applicable in any state where one wishes to make or receive bets. However, there are two federal laws that serve to restrict online gambling. First, in the case of *In re MasterCard International, Inc. Internet Gambling Litigations*, the Fifth Circuit Court of Appeals held that the Federal Wire Act of 1961 prohibited the transmission of information for sports betting across telecommunication lines, but that this law did not prohibit 'internet gambling on a game of chance'. In response to this holding, Congress passed the Unlawful Internet Gambling Enforcement Act (UIGEA). While the UIGEA does not expressly ban online gambling, it prohibits 'gambling businesses from knowingly accepting payments in connection with [...] a bet or wager that involves the use of the Internet and that is unlawful under any federal or state law'. The UIGEA also imposed restrictions on institutions involved in the transfer of funds to facilitate gambling activities. As a result, most publicly traded internet gambling companies stopped taking bets from US citizens shortly after the UIGEA's passage, and several online poker companies were subjected to criminal investigations related to, among other things, their concealment of funds transfers from US players. While there have been some efforts to treat online poker sites differently than other online gambling sites, to date there has been little to no movement on this issue in Congress. Fantasy sports, games of skill, and legal intrastate and intertribal gambling are expressly exempted from the UIGEA. In recent years, companies like Draft Kings and FanDuel have sought to take advantage of the 'fantasy sports' exception to allow users to bet on the outcome of fantasy sports. While many states initially responded by actively outlawing daily fantasy sites or filing lawsuits against these companies for violating state gambling laws, the legality of daily fantasy sites has recently become a hot-button issue in jurisdictions across the US, and there appears to be a trend across the US towards the legalisation of daily fantasy sites. There are now 11 states that have passed laws expressly legalising daily fantasy sports in some manner, nine of which have been passed in the past two years, and many others have legislation pending that would legalise such sites. However, to date, these sites remain outlawed in eight states, and additional states continue to evaluate their legality or are involved in ongoing negotiations regarding their operation. Thus, in states in which laws have not been passed legalising daily fantasy sites but where these sites nevertheless continue to operate, the continued legality of their operations remains uncertain.

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

As noted above, the legality of online gambling and associated verification requirements are entirely a function of state law. States that permit online gambling typically impose requirements that sites verify age, credit and other factors.

Outsourcing

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

Some of the legal and tax issues relevant to outsourcing include intellectual property (ownership and protection), the scope of services, performance, pricing and exculpatory scheme. Numerous federal and state laws apply to outsourcing, including (i) Sarbanes-Oxley Act of

Update and trends

IoT

IoT signifies the interconnection via the internet of computing devices in everyday objects (eg, cellphones, watches, washing machines, headphones, and lamps), enabling them to send and receive data. Some of the major privacy concerns created or exacerbated by the rise of IoT include continuous collection and communication (including ambient collection), inadequacy of user notice and choice, confidentiality and data security, and data aggregation.

The majority of IoT devices do not provide effective notice of privacy policies to the end-user, in large part because many lack an adequate display surface for such policies. In an effort to ameliorate this issue, some manufacturers and researchers are developing creative ways to provide notice through secondary channels, such that consumers receive privacy policy notices via email, text message or even haptic media to warn that certain functions are enabled. However, notice and consent issues are particularly salient in public places. Every IoT device can be tracking a variety of different people around them when used in public, raising privacy concerns for unknowing bystanders (even though the individual end-user has given consent).

Cybersecurity is one of the most pressing problems in the IoT space, both for the technological and for the legal challenges it poses. Given the ubiquity of internet connectivity as a heavily marketed feature in the consumer electronics market today, inadequate IoT cybersecurity substantially increases the attack vectors available to hackers against targets. The complex supply chain for technology products exacerbates the problem significantly. For example, chipset manufacturers may hardcode (so future users cannot change) admin credentials (functionally serving as a manufacturer 'backdoor') into their software, and if those credentials are identical across a range of IoT devices, then all of them are potentially vulnerable to the same exploit. Hostile actors have already been exploiting these vulnerabilities with massive impacts (eg, the DDoS cyberattack on DNS provider Dyn in October 2016 that caused outages on several of the most popular websites and platforms, including Amazon, Airbnb, GitHub, PayPal, Netflix, Twitter, Spotify and The New York Times).

Despite recent security breaches, the PEW Research Center reported that the connectivity between humans and IoT devices will become more prevalent in the upcoming years. In particular, millennials continue to crave convenience over cybersecurity risks. As developers continue to roll out new and different IoT devices, various players in the private and public sector have started to pinpoint issues and craft industry-wide solutions regarding the privacy and data security issues surrounding IoT.

Blockchain

Blockchain, the distributed ledger technology underlying the cryptocurrencies Bitcoin, Ethereum, Litecoin, and a host of others, is becoming increasingly integrated into the digital economy, and has the potential to transform the ways in which individuals and businesses engage in business.

Generally speaking, a blockchain is a database of digital transactions distributed across an open and decentralised peer-to-peer network. The authenticity of each transaction in the database is verified by participants in the blockchain network and recorded in a linear and chronological order. Before a transaction can be added to the blockchain, the participants in the network must verify the authenticity of the transaction. Once verified, a transaction is time-stamped and added to the blockchain, and thereafter cannot be removed or altered. As a result of its open, distributed, and unalterable nature, blockchain offers a mechanism for recording, tracking and verifying assets and information that is more efficient, transparent and secure than traditional means, without the need for an intermediary to verify the transaction.

Given blockchain's history as the technology underlying cryptocurrencies, it is no surprise that the financial industry has shown the most avid interest in blockchain technology to date, with the majority of the world's leading financial institutions focusing more attention and investing more heavily in the development of blockchain technology each year since its inception. However, companies in a variety of other industries (healthcare, fashion, manufacturing, entertainment, telecommunications, etc) have begun exploring potential applications of blockchain technology (eg, use of blockchain to improve internal business processes, including supply chain management). One application of blockchain technology that has recently garnered attention is its use in connection with 'smart contracts', or contracts that are written and recorded in computer code, the terms of which are capable of being executed and enforced in an automated fashion when certain conditions are met. In addition, US federal and state governments have begun exploring applications for blockchain: in December 2016, the Federal Reserve Bank in the US for the first time officially commented on blockchain technology by releasing a research paper in which it explored potential applications of blockchain technology; similarly, several states have unveiled blockchain initiatives in the past year that are aimed at exploring applications of blockchain technology.

Often described as the most significant technology to be introduced since the invention of the internet, the increasing interest in blockchain technology across all sectors comes as no surprise. While applications of blockchain technology have rapidly multiplied since it was first introduced nine years ago, it seems that users have only begun to scratch the surface of its potential applications. However, one thing seems certain: blockchain is here to stay, and will likely continue to become a more integral part of everyday life.

2002 (which contains provision with respect to the retention of emails, data security and oversight) that should be considered when outsourcing data to the cloud; (ii) PCI DSS; (iii) HIPAA; and (iv) GLB. The attendant legal issues with respect to outsourcing a service will often depend on the nature of the service being outsourced. For example, cybersecurity and compliance with data privacy legislation are important where an organisation is transitioning to cloud computing. Moreover, certain data security requirements must apply throughout the whole supply chain. If financial services are being outsourced, compliance with the Sarbanes-Oxley Act is a key concern. If an outsourcing arrangement involves the hiring of staff, certain US laws with respect to the transfer of employees may apply. Offshore outsourcing may involve the laws of another jurisdiction in addition to laws with respect to cross-border data transfers. In brief, the nature of the services being outsourced and the location of the service provider should be carefully considered to effectively navigate the regulatory landscape.

46 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?

Most employment laws in the US are promulgated by state and local entities. However, if there is going to be a layoff above a certain threshold, the federal Worker Adjustment and Retraining Notification Act (the WARN Act) requires covered employers with 100 or more employees to provide 60 days' advance notice of a layoff that affects a certain number of or percentage of employees so that the affected employees have the opportunity to seek employment elsewhere. The WARN Act carves out exceptions for companies that (i) are actively seeking capital or new business; (ii) encounter unforeseeable business circumstances; and (iii) are forced to close or lay off employees as a direct result of a natural disaster. In addition, some states, including California, Maine, New York, Pennsylvania and Wisconsin, have enacted their own versions of the WARN Act (referred to as the mini-WARN Acts).

Online publishing

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

As noted above, websites and web services that passively host third-party content are generally immunised for content posted on their sites under by section 230 of the Communications Decency Act. Indeed, recent case law even suggests that websites like eBay are not liable for counterfeit goods sold via online marketplaces, and that trademark owners are responsible for policing such conduct and notifying eBay to request the removal of such goods. *Tiffany (NJ) Inc. and Tiffany and Company v eBay Inc.* As such, companies concerned about counterfeit goods should implement active policing programmes to identify misconduct and to notify online sellers. Further, as noted above, in some cases counterfeiting cases can be successfully referred to federal authorities. However, content and data providers are subject to the same liability (and First Amendment protections) as traditional print media for errors included in content they create.

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

Copyright protection vests even in works that display a modicum of creativity, including databases of information. *Positive Software Solutions, Inc. v New Century Mortgage*. However, this protection only extends to the database itself rather than the underlying information contained within that database. Moreover, factual compilations like databases are typically only provided 'thin' protection, meaning that in many cases only wholesale appropriation may constitute infringement. *eScholar, LLC v Otis Education Systems, Inc*. Websites that are seeking to protect their databases are advised to notify visitors that their databases are copyrighted materials (eg, through the use of a copyright notice), and to use comprehensive click-through agreements (as discussed above) to strictly limit access to, and use of, their databases. In this manner, websites can secure contract rights above and beyond the scope of their copyright protection to pursue those that improperly use or reproduce their works.

KIRKLAND & ELLIS

Gregg Kirchhoefer **gregg.kirchhoefer@kirkland.com**
P Daniel Bond **daniel.bond@kirkland.com**
Ashley Eisenberg **ashley.eisenberg@kirkland.com**
Adine Mitrani **adine.mitrani@kirkland.com**

300 North LaSalle
Chicago, IL 60654
United States

Tel: +1 312 862 2000
Fax: +1 312 862 2200
www.kirkland.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

e-Commerce
ISSN 1473-0065

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law