e-Commerce

Contributing editor
Robert Bond

2017

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

e-Commerce 2017

Contributing editor

Robert Bond

Charles Russell Speechlys

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
Thirteenth edition
ISSN 1473-0065

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

CONTENTS

United States

Gregg Kirchhoefer, P Daniel Bond and Shannon Yavorsky
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 progressive initiatives, policies and engagements that are aimed at: expanding access to the internet; ensuring that the internet remains open and free; and preserving and protecting cyberspace.

As to access to the internet, in 2009, the US government earmarked $7 billion in investments from the Recovery Act to expand broadband access through the US, improve high-speed internet connectivity in rural areas and 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.

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 to, among other things, promote and 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.

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.

The US government recognises 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 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 forgoing 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 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 internet service provider;
- 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;
- 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 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 touch information and sets out standards that apply to the electronic transmission of medical data;
- the Electronic Communications Privacy Act: 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: governs computer hacking and makes unlawful certain computer-related activities involving the unauthorised access of a computer;
- the Communications Decency Act of 1996: 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 trademarks owners against a person who registers, traffics in, or uses a domain name that is identical or confusingly similar to the mark or, in the case of a famous mark, dilutes the mark and has a bad faith intent to profit from the trademark;
- 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 (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: 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;
- 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/slow lanes to content);
- the Prioritizing Resources and Organization for Intellectual Property Act of 2008: increases both civil and criminal penalties for trademark, patent and copyright infringement, including online infringement; and
- 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, 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, while not yet in force, certain provisions of the European General Data Protection Regulation will apply to businesses if they offer goods or services to data subjects in Europe or monitor data subjects' behaviour in Europe.

Regulatory bodies

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

The regulatory bodies are:
- the Federal Trade Commission (FTC): regulates e-commerce activities, including online advertising and consumer privacy;
- the FCC: regulates interstate and international communications by radio, television, wire, satellite and cable, including telecommunications across the internet;
- 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; and
- the Advisory Commission on Electronic Commerce: created by Congress to study federal, state, local and international taxation and tariffs on transactions using the internet and internet access.

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 members to adopt authentication systems for outgoing email. 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).

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 the decisions of an out-of-state court without having 'purposely availed' himself 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 that articulate the circumstances in which personal jurisdiction may be asserted in an internet context. Certain courts distinguish between active and passive websites and will extend jurisdiction over the proprietor of a website that actively markets to customers in a particular jurisdiction (as opposed to a passive website that does not purposefully interact with individuals in a particular jurisdiction).

The traditional test of personal jurisdiction arose out of the case of *International Shoe v Washington*, 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 in which 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 meet the interactivity of minimum contacts needed for personal jurisdiction.

Other courts look to the 'sliding scale' or Zippo test from *Zippo Manufacturing Co v Zippo Dot Com, Inc*, in which a 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'.

Further cases assist in providing guidance in specific circumstances, for example, in *Pres-Kap, Inc v System One, Direct Access, Inc*, the 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 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*, a court held that a passive web page, that did not advertise in Arizona, was not enough to establish personal jurisdiction in Arizona. 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). But 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 accepts the proposed terms. In many cases, a site may require users to either scroll through their proposed terms or check a box affirming they have 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 '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 their 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 were located down the page from the download button and the user was not required to affirmatively indicate their 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 business, 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*). But 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.

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 check a box indicating they have reviewed the same via a link in direct proximity of that box. Third, a user should be required to confirm that they are 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. 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 they have initially formed a contract 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:

- wills, codicils and testamentary trusts;
- laws governing domestic law matters;
- state Uniform Commercial Codes, except sections 1-107 and 1-206, articles 2 and 2A;
- court orders and notices;
- utility cancellation notices;
- default, foreclosure, or eviction notices;
- health or life insurance benefit cancellation notices;
- product recall notices; and
- hazardous, toxic, or dangerous materials notices.

The ESIGN Act does not distinguish between business-to-consumer and business-to-business contracts; 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 (the 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 sales 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.

Finally, the Uniform Computer Information Transaction Act (the 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 '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. Moreover, in 2003 the American Bar Association withdrew its prior approval of the UCITA as a uniform law provision. Thus, while the UCITA may have impact in Maryland and Virginia, its provisions have been roundly rejected (or affirmatively thwarted) by most state governments.

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 comments. 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 businesses maintain records regarding the precise circumstances regarding any express or implicit consent they 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, HIPAA, the GLBA, 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. 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, 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. 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 which 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) is a uniform information security standard for organisations that handle credit cards, which was formed by Visa, MasterCard, American Express, Discover and JCB. 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, the GLBA), 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 *re Boucher*, the court ordered an individual to produce the password to the individual's hardrive 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 help the US Department of Justice 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. 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. As of June 2016, there is a case pending before the US Court of Appeals for the 3rd Circuit on the Fifth Amendment limits of forcing a suspect to enter his password to decrypt a computer. The decision in this case may provide further clarity on this issue. 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 they need to provide evidence and develop detailed specifications for what the exceptional access mechanisms are expected to do.

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 a top-level domain (TLD) registry. The Internet Corporation for Assigned names and Numbers (ICANN) is responsible for bestowing accreditation on non-country-specific TLD registrars (.com, .ne, 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 a registration of a '.us' domain name, which are centred around the registrant having a sufficient US nexus and bona fide presence in the US. One of the following three territorial requirements must be satisfied in order to register a country-specific domain name: registrant must be a US citizen or permanent resident, with primary domicile in the US; registrant must be an entity incorporated in the US; or registrant must be a foreign entity with 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 as a trademark. The domain name owner can thus develop common law rights in the domain name, which may become capable of registered trademark protection.

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 ACPA for abusive use of domain names. The owner of a trademark can use evidence of ownership to show that a domain is identical or confusingly similar to his or her trademark; the domain name was registered in bad faith; and 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 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 conventional and online advertising, both via government action and civil claims from competitors, consumers and even putative classes. Thus, online advertising must be subject to the same stringent controls that organisations employ 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) 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 like 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 preempts any such legislation, and the statute itself purports to 'supersede[] any statute, regulation, or rule of a State . . . that expressly regulate[] 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 rules regarding the sending of commercial email and text messages to wireless devices. For commercial emails sent to wireless devices: a recipient must consent to receive such emails in writing; the sender must identify the name of the entity sending the messages and the entity advertising products and services; and the sender must provide an opt-out that allows recipients to opt-out the same way as 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 is agreed to receive advertisements to their wireless device, the identity of the advertiser, 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 keenly aware of the potentially devastating impact that violations of the Telephone Consumer Protection Act (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 facsimile an existing business relationship may permit faxing if FCC-proscribed opt-out language is included). Notably, the TCPA provides for damages of $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 recent years, Capital One agreed to a settlement of $75.5 million over claims related to autodialled calls to cell phones, and Jiffy Lube agreed to a settlement valued at between $35 and $47 million for a text message promotional claim. 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, and 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 children less than 13 years of age. Prior to the collection of 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 reasonably necessary. In addition, since 2013 the FCC has made clear that COPPA applies both to a website and any outside services (eg, plug-ins like 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.

Finally, private industry groups like 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. The 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 Food and Drug Administration (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 and 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 keenly 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 formal 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 immunity 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*). However, there is very little guidance on where the line is drawn between advertising and editorial content, meaning that companies should be very mindful of the potential implications of their online publishing, particularly as 'advertorial' content becomes a common revenue stream for many websites.

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, '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. 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 of the Communications Decency Act.

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 via the internet is highly regulated in the US. To begin with, the same consumer protection laws that apply to advertising other products and services also apply to the online advertising of financial services products. For example, under the FTCA, advertising must be truthful and non-deceptive, must be substantiated and cannot be unfair. As to laws which 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, 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 Securities and Exchange Commission (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 measures to regulate crowdfunding (a method of raising capital that is used to raise money on the internet).

Defamation

20 Are ISPs liable for content displayed on their sites?

ISPs are generally not liable for materials posted on their sites. Section 230 of the Communications Decency Act of 1996 (Title V of the Telecommunications Act) 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 definition of 'interactive computer service' 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 disincentivising efforts by ISPs and other online service providers to monitor user content without subjecting themselves to 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 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 post questionnaires including mandatory, pre-populated answers may be '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 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.

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: the purpose and character of the use; the nature of the copyrighted work; the amount and substantiality of the portion taken; and 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*, a 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. In *Author's Guild, Inc v Google, Inc*, a 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* a court held that posting an entire editorial from a newspaper as part of an online discussion constituted fair use. However, 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. Finally, 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*).

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 a person or entity 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 trademarks in the domain name of 'gripe sites' designed to criticise a company (*Ford Motor Co v 2600 Enterprises*). The use of a trademark on a site has been found to infringe where it is used to market competing goods or to direct consumers to sites where they can make purchases from competitors (*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 (*Digital Equipment Corp v AltaVista Technology*), but that linking to another website does not (*Ticketmaster Corp v Tickets.com, Inc*). But 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 programmes 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 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 from a third party to build their site, they 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 for 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 (*Viacom Intern, Inc v Youtube, Inc* and *IO Group v Veoh Networks, Inc*). However, courts have held that owners of a website can be liable if they post links to infringing materials in contravention of an injunction. Moreover, 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*).

As discussed at length 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*). But 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?

Generally speaking, TV content is 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 Deceny 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 stations at any time and the airing of 'indecent' material between 6:00 AM and 10:00 PM. However, this standard only focuses on 'material that describes or depicts sexual or excretory material,' and not 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. 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 National Intellectual Property Rights Coordination Center 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, which are a form of intellectual property, and other forms of industrial espionage, and provides the ability to seize appropriate materials and enjoin further violations of the act. In general, injunctions against copyright, trademark and patent infringement are primarily provided via civil rather than criminal lawsuits. 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 United States International Trade Commission (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 which regulate the collection, use, processing, disclosure and security of personally identifiable information (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, and importantly, 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. 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?

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 (the 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 which 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. As a consequence, transfers of personal data from the EEA to the US have to be made on the basis of another approved mechanism for cross-border data transfer. The key remaining mechanisms under the Directive for such transfers are binding corporate rules and standard contractual clauses.

Notably, the European Commission and US authorities proposed a replacement for Safe Harbor, the 'EU-US Privacy Shield', but at the time of writing, this measure is the subject of criticism and not yet in force. Further, the General Data Protection Regulation (GDPR), that 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 impact 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, but 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. 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 which includes a term that the organisation will not sell PII, the organisation must comply with that term.

California's financial privacy law (Cal Fin Code sections 4050-4060) prohibits sharing or selling personally identifiable non-public financial information without consent. Additionally, under recent Californian 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.

Under HIPAA, there are criminal penalties of up to $250,000 and 10 years' imprisonment if the offence was committed under false pretences or with intent to sell the data for commercial gain.

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 which 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 laws?

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.

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.

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

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

The Telephone Consumer Protection Act of 1991 (TCPA), restricts the use of automated telephone equipment (auto diallers) and requires prior express written consent for: 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 pre-recorded telemarketing calls to residential lines.

There is also a Telemarketing Consumer Fraud and Abuse Prevention Act and Telemarketing Sales Rules, which prohibit any deceptive telemarketing acts. The TCPA also prohibits: sending commercial advertisements to a person or business by fax; and auto-dialled texts to wireless numbers (unless the caller receives the prior written consent of receiver).

The CAN-SPAM Act governs unsolicited 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. 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 $400,000 for sending email with misleading headers and deceptive subject lines and without an opt-out mechanism or valid physical postal address (*FTC v Cleverlink Trading Ltd*).

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

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?

Individuals have to be notified under various state laws in the event of a data breach. In addition, under HIPAA, certain entities, including healthcare providers must notify individuals when their unsecured health information has been breached. In addition, national banking regulators have issued guidance encouraging financial institutions to notify customers if the institution identifies misuse of customer information.

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).

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 the 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 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). Some states also 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. The Marketplace Fairness Act is legislation currently pending in the United States Congress, which would require state governments to collect sales taxes and use taxes from out-of-state retailers with no physical presence in their state.

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 in question 39 for imposition of sales tax in the state where the server is located. Some states like 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 in question 39 where there is taxable nexus.

Update and trends

Social media usage

As more companies seek to use social media to advertise to, and engage with, their customers, they have found themselves exposed to significant additional risk of litigation. Recent cases have found that companies can potentially be liable for trademark infringement if they adopt Twitter handles or hashtags that could result in consumer confusion (*Public Impact, LLC v Boston Consulting Grp, Inc* and *Fraternity Collection v Fargnoli*). Indeed, the United States Patent and Trademark Office has granted over 100 trademark registrations for hashtags in just the past two years. Companies are also increasingly facing right of publicity violations when they use images of celebrities over their social media accounts (*Heigl v Duane Reed, Inc*). This liability could even theoretically extend to efforts to invoke the identity of a celebrity, even if they are not depicted in an advertisement or social media post (*Jordan v Jewel Food Stores, Inc*). Because publicity rights vary widely from state to state, companies should be mindful of the locations in which online advertising may appear since numerous jurisdictions may be implicated. Moreover, the increasing number of fake accounts on social media requires companies to protect their trademark rights by carefully monitoring social media for unapproved or misleading uses of their trademarks. This also requires companies to be keenly aware of the policies of social media companies like Facebook and Twitter regarding false or misleading 'squatter' accounts.

Finally, companies should be mindful that social media creates potential risk for companies that are too aggressive in asserting their rights online. For example, Goldman Sachs recently found itself subject to a wealth of bad publicity and a declaratory judgment action in Florida after it threatened to sue a critical site called goldmansachs666.com. In the age of social media, there is always a risk that over-aggressive companies may find their actions have gone viral, generating far worse publicity than the original conduct at issue. Similarly, the New York Times faced considerable online criticism (and inadvertently drew attention to a critical parody account) when it filed a trademark complaint against the Twitter account @NYTOnIt. Thus, both legal and marketing considerations must be carefully weighed as companies enforce their rights online. Nonetheless, companies have had success in attacking imposters outside the context of criticism and parody accounts and should address efforts to hijack their brands, particularly given their duty to police the use of their marks (*Nine West Development Corp v Does 1-10*).

Employer access to social media user names and passwords

Since 2012, states have increasingly banned efforts by employers to require employees to turn over their usernames and passwords for personal or social media accounts. To date, 23 states (and Guam) have implemented laws banning or limiting this practice, and numerous states are currently considering similar litigation. These laws may extend to employees, students and, in some jurisdictions, even tenants. Penalties can include criminal liability, monetary damages, injunctive relief, and in some states even attorneys' fees and costs. Companies seeking such information from their employees should carefully analyse whether this practice is permitted in the states in which they reside. Moreover, recent cases have suggested that accessing the personal accounts of an employee may constitute an invasion of privacy or the infliction of emotional distress (*Mintz v Mark Bartelstein & Accossiates* and *Murphy v Spring*). Further, the National Labor Relations Board is increasingly taking notice of employers that monitor employee social media activity or blogging in the context of National Labor Relations Act investigations (*Triple Play Sports Bar & Grille v Purple Communications*).

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. It is important to consult an appropriate tax specialist given the complexity of this issue. If the transfer price for the goods returned to the onshore company are unreasonably higher than the costs paid by the 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 will 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 held that the Federal Wire Act of 1961 prohibited the transmission of information for sports betting across telecommunication lines. But the court also ruled that this law did not prohibit 'internet gambling on a game of chance'. In response to this holding, Congress passed the 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 sought to take advantage of the 'fantasy sports' exception to allow users to bet on the outcome of fantasy sports. However, many states have responded by actively outlawing daily fantasy sites or filing lawsuits against these companies for violating state gambling laws. To date, 11 states have outlawed these sites, though additional states continue to evaluate their legality or are involved in ongoing negotiations regarding their operation. Thus, even in states where daily fantasy sites 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: the Sarbanes-Oxley Act of 2002 (which contains provision with respect to the retention of emails, data security and oversight) which should be considered when outsourcing data to the cloud; PCI DSS; HIPAA; and GLBA. 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. If financial services are being outsourced, compliance with SOX 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 transfer. 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.

With respect to tax, it is important to ensure that the deal is structured to be both tax efficient and comply with all applicable tax laws. It is critical to consult a tax specialist, particularly if a multi-jurisdictional outsourcing is at issue.

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, the federal Worker Adjustment and Retraining Notification Act (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. In addition, some states have enacted their own versions of the WARN Act (also referred to as 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 by section 230 of the Communications Decency Act for content posted on their sites. 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. As such, companies concerned about counterfeit goods should implement active policing programmes to identify misconduct and 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 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 work.

KIRKLAND & ELLIS

Gregg Kirchhoefer **gkirchhoefer@kirkland.com**
P Daniel Bond **dbond@kirkland.com**
Shannon Yavorsky **syavorsky@kirkland.com**

300 North LaSalle
Chicago, IL 60654
United States

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