TechTarget

Where serious technology buyers decide

A TechTarget Global Marketer Services White Paper:

Global Technology Marketing and the Law

Best Practices Collection

Making Sense of Regional & Country-Specific Requirements for Online Marketing

Gina Perini, GTC Law Group LLP, in collaboration with TechTarget

Introduction

Online marketing provides vast opportunities for technology marketers to better understand prospective customers by collecting and sharing information from and about users. However, given the inherent privacy concerns, governments, industry groups and regulators have responded with a myriad of new and ever-changing rules, regulations and guidelines that present marketers with the challenge of understanding what they can and cannot do, particularly when launching campaigns in new markets or running campaigns across multiple countries bound by different laws.

Not surprisingly, the specifics of these regulations vary greatly from country to country. Making matters still more complicated, laws of jurisdictions often overlap, requiring marketers to simultaneously comply with multiple, and sometimes conflicting, regulations. As a result, a global online marketing campaign often requires a marketer to navigate a regulatory minefield in which errors in guidance or execution can lead to embarrassing, and potentially costly, missteps.

The purpose of this white paper is to educate global technology marketers and help them navigate this regulatory maze in order to maximize the success of their marketing efforts while complying with applicable requirements.

Specifically, it will walk you through the legal frameworks applicable to online marketing and provide practical marketing advice related to the following areas:

- Data protection
- Online advertising and website marketing
- Email marketing
- Mobile marketing
- Telemarketing
- Laws and regulations applicable to content development and messaging (including comparative advertising)
- Emerging markets

Contents

Introduction 2

Data protection laws to consider 3

Online advertising and website marketing 4

US-EU Safe Harbor certification 5

Email marketing 6

Mobile marketing 7

Telemarketing 8

Laws and regulations applicable to content development and messaging 9

Emerging markets 11

Glossary of terms 12

While the intent of this paper is to give you an overview of common laws and guidelines regulating online marketing in various global regions, it is strongly advised that you consult local counsel about your specific marketing campaigns to determine the practical application of the laws outlined.

Data protection laws to consider

One of the fundamental areas of online marketing regulation is a category of laws[1] known as "data protection" laws. These laws regulate the collection, use, storage, disclosure, and other processing of "personally identifiable information" or "PII". There are various approaches to regulation globally, but most fall into two categories: the US Federal regime, which is sector-specific and data-specific, and the EU regime with all-encompassing privacy laws applicable to all PII, regardless of sector, category of individual, or type of PII.

- **US.** In the United States, federal data protection focuses on industry sector, with a comparatively thin over-lay of general regulation by the Federal Trade Commission (FTC). In connection with digital marketing, there are a variety of statutes individually regulating such diverse activities as email marketing (CAN-SPAM Act of 2006) and telemarketing (the FTC Do Not Call Registry). Although there is currently no wide-sweeping federal privacy law, the FTC has enforced data protection rights under the consumer protection regulations of the Federal Trade Commission Act. In addition, there are several bills in Congress that would, if enacted, implement a more general regime for US Federal regulation. Within individual states, regulation tends to be less sector-specific and closer to the EU model of general rules governing all PII. Unfortunately, there is no guiding principle or set of policies that informs and coordinates the various state laws in the US.
- **EU.** The European Union (EU) data protection regime is, in general, broader, more restrictive and more consistent than the regulatory landscape in the US. EU regulation begins with an overarching privacy directive applicable to the processing of all types of personal data (Data Protection Directive). Unlike the sector-specific definitions of PII found at the Federal level of US regulation, the definition of PII under the directive applies to any data that can be linked with an "identified or identifiable person" including email addresses and IP addresses. EU member countries have implemented the Directive with additions and modifications that, in some cases, further restrict data collection and use.
- **Other markets.** Other markets around the globe often are modeled after either the US or EU regimes, or a combination of both, with most recent regulation favoring the EU model.

Key takeaways for marketers

If you are targeting a specific country's citizens, you should comply with that country's data privacy regulations. The main considerations that may impact which regulations apply include:

- Target audience location;
- The languages being used;
- The types of data you will be collecting; and
- Where the data will be stored

If you structure campaigns to run across numerous countries, you should at a minimum make sure you comply with the laws of the most restrictive country and any specific data protection requirements of each country. In all instances, any third-party

If you structure campaigns to run across numerous countries, you should at a minimum comply with the laws of the most restrictive country and each country's specific data protection requirements.

[1] For convenience, this paper will, unless otherwise stated, use the term "law" to refer to directives, statutes, regulations and other governmental acts having the force of law.

vendors or partners who may deploy such campaigns on your behalf should also address and comply with these laws.

Online advertising and website marketing

The increased market reach provided by the Web also increases the need for complying with different regulations across the globe. Additionally, the emergence of sophisticated marketing automation (e.g. Marketo, Eloqua) and behavioral tracking platforms used either on your own website and/or across third party publisher websites and ad networks, means that data collected about a user's behavior during their visit is also subject to data privacy regulations in many nations.

Although many countries apply existing advertising regulations to the Web, others have enacted regulations that specifically target this type of marketing. In the major markets, we find a continuum of approaches:

- **US.** The United States has not enacted laws to specifically regulate online marketing, but instead businesses must navigate a patchwork of state and federal consumer protection laws to ensure compliance. (For instance, the FTC and state consumer protection agencies are charged with, and enforce, a myriad of consumer protection regulations related to advertising.) The FTC has recently made recommendations to create a sweeping law to address online marketing. If adopted, these regulations would require companies to restrict information collected from users to only what is necessary to carry out a particular transaction and would prevent companies from retaining that information longer than is necessary to complete the transaction. Further, the regulations would require companies to clearly identify to users what and how personal data is being collected and provide meaningful choices on which types of data can be collected from their online activities. In addition to governmental regulation, there are also self-regulatory guidelines that industry organizations have promoted to address user and governmental concerns about online marketing. For instance, in the US, the Digital Advertising Alliance has promulgated a self-regulatory program to address online marketing. Although these guidelines do not carry the force of law, marketers may find that their customers and their partners are mandating that these best practices be adopted.
- **EU.** In the European Union, marketers are more limited in their ability to advertise online than in any other jurisdiction. The EU Directive on Privacy and Electronic Communications places significant restrictions on when and how advertisers may collect information from users. For instance, information may only be retained so long as it is necessary to communicate with, or bill, the user, unless the user gives his or her consent otherwise. Probably the most talked about and challenging requirement, however, is the requirement that online advertisers obtain consent before they store information, such as cookies, on the computers of users, and that consent must be given after a full disclosure of the purpose of the storage.[2]
- **Other Markets.** In Australia, New Zealand, Brazil, India, Russia and China, there are no regulations in place targeting online marketing. In these nations, online advertisers must comply with those regulations that apply to offline advertising, such as consumer protection and truth in advertising laws.

[2] UK's Information Commissioner's Office (ICO) has issued guidance on its approach to enforcing the Privacy and Electronic Communications Regulations (the "Regulations"), which came into effect on 26 May 2011; *see* http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx. The ICO guidance confirms that the UK Communications Commissioner will allow a lead-in period of 12 months for organizations to develop ways of meeting the cookie-related requirements of the Regulations before he will consider using his enforcement powers. However, the ICO has stated that it will not condone organizations taking no action in the period up to May 2012 and may issue warnings if particular organizations are not making adequate preparations to be compliant by then.

Key takeaways for marketers

A marketer's major considerations can be summarized as:

- **Website privacy policies**—these must be kept up to date with the evolution of data privacy regulations and should clearly and succinctly describe how data is collected, used, and disclosed to users who visit your website(s). Periodically, and before any change is made in the way you collect data about users who visit your website(s), you should review and update your privacy policy to reflect your current practices.
- **Opt-in considerations and behavioral tracking**—in countries where you must obtain consent (e.g., "opt-in") before you collect online behavioral data about users, you should ensure that the way you obtain consent is compliant with the applicable law. Be especially careful when targeting the EU, as some EU countries may require you to obtain consent before placing cookies on users' devices.
- **Leveraging third parties**—when using third parties to deploy online advertising on your site (e.g., ad networks and marketing automation tools) you must also ensure that they are in compliance with applicable law, including providing any required privacy notices and obtaining any required consents, and that such obligations are included in your **contracts with these third parties.**

In countries where you must obtain consent (e.g., "opt-in") before you collect online behavioral data about users, ensure that the way you obtain consent is compliant with the applicable law.

US-EU Safe Harbor certification

Given the EU's directives regulating data privacy and the transfer of PII from the EU to entities abroad, online advertising practices engaged in by companies outside of the EU, and in particular in the United States, often violate EU law. In fact, the EU has found that the US regime does not have adequate laws in place in connection with PII protection that are sufficient to meet regulatory standards unless the entity transferring the data from the EU to the US (including storing the data on US servers) is self-certified under the US-EU Safe Harbor Framework or takes other steps allowed under the EU Data Protection Directive.

Administered by the US Department of Commerce, the US-EU Safe Harbor Framework[3] is a self-certification program that allows for the transfer of data from the European Economic Area to the US as long as the receiving entity complies with a set of stated principles. These principles ensure that the PII is only collected from individuals that have given their informed consent based on prior notice as to the purpose of the collection, and that the data will be handled securely and responsibly.

The process of filing the self-certification form under the Safe Harbor Framework is quite simple. The real work will be the internal assessment by your company beforehand to ensure that you comply with the Safe Harbor principles and take any steps necessary to become compliant.

It is important to recognize that the Safe Harbor framework is not merely window-dressing for data transfers. The FTC has taken an active interest in companies' compliance with their representations to their customers about data protection and use. If a company certifies that it is Safe Harbor Framework compliant, but then violates the Safe Harbor principles, it exposes itself not only to civil liability to individuals whose PII has been misused, but also to regulatory action by the FTC and, in some cases, the EU data protection authorities.

[3] Detailed information and online forms to self-certify to the US- EU Safe Harbor Framework found at http://export.gov/safeharbor/eu/index.asp.

Key takeaways for marketers

For US marketers that wish to target users in the EU, you will want to make sure that your organization is self-certified under the Safe Harbor Framework before running digital campaigns. Further, marketers should make sure that their marketing and media partners are certified under the Safe Harbor Framework—as TechTarget is—if they collect information about EU citizens that will be **stored, used or shared in the US.**

Marketers should make sure that their marketing and media partners are certified under the Safe Harbor Framework if they collect information about EU citizens that will be stored, used or shared in the US.

Email marketing

Just as there are a number of regulatory schemes in place covering online marketing, there are also a number of schemes that govern the practice of direct marketing by means of email. Additionally, a number of jurisdictions place unique restrictions on the specific subject matter of the email and how it must be labeled.

In a global environment it can be challenging to tailor marketing campaigns to the laws of each particular jurisdiction. It is often impossible to verify the physical location of the person to whom the email is being sent; furthermore, people are highly mobile and can easily move from one jurisdiction to another while retaining the same email address. Under these circumstances, it is tempting to adopt a 'lowest common denominator' approach, in which all email marketing is made to comply with a combination of the most restrictive requirements. This can deprive the marketer of valuable opportunities in less restrictive jurisdictions. One must carefully balance the risk of an inadvertent violation in more restrictive jurisdictions against the benefits accorded by the more liberal environments.

In the major markets, we find that all email marketing (regardless of industry) requires:

- **US.** In the US, email marketing is governed by the CAN-SPAM Act of 2006, which requires advertisers to provide email recipients with the option to opt out of receiving future advertisements. Steps must also be taken to remove any users who have opted out of your mailings from third party lists that are purchased. Finally, any direct marketing email must contain an address for contacting the sender and may not contain any misleading information in the header or subject line.
- **EU.** In the EU, email marketing is addressed primarily by the EU Directive on Privacy and Electronic Communication. Member nations require that direct marketing by email only be sent to those users that have given prior consent (known as, "opt-in") to receive such emails; opt-ins may not be pre-selected for users on your websites. Consent is not required where the recipient's email address was acquired through the sale of goods and services, however, all emails must contain contact information to allow recipients to inform the sender if they wish to opt out of receiving future emails. There are some nations within the EU that have further requirements beyond the scope of the Directive on Privacy and Electronic Communication making additional analysis necessary. Countries such as Germany also require one to obtain a "double opt-in" by means of sending a confirmatory email to the user in order to confirm that such user has consented to the collection, storage and use of their PII and receiving marketing email communications. The European Commission has passed legislation in the revised E-Privacy Directive that gives users and private organizations the right to sue spammers for unsolicited commercial emails. In particular, this would enable ISPs and consumer protection organizations to take action against spammers.

- **Australia.** In Australia, email marketing is governed by the Spam Act of 2003, which prohibits sending direct marketing emails to users who have not given prior consent (opt-in) to receive such emails. However, consent can be inferred from the existence of a prior business relationship between the parties, or by publicly accessible publication of the recipient's business email address. The Act also requires that such emails contain an address to which recipients may send requests to opt out of receiving future emails.
- **China.** In China, email marketing is governed by the 2006 Regulations on Internet Email Services, which prohibit the sending of direct marketing emails to users without their prior consent (opt-in). The Regulations apply to any email containing any advertising content, even if the email is not primarily intended as an advertisement. Such emails must be labeled as an advertisement in their subject lines.
- **India.** In India, there is currently no law or regulation governing email marketing.

Key takeaways for marketers

The spectrum of regulations governing email marketing is broad, ranging from a complete lack of regulation to very restrictive double opt-in requirements. Figuring out which laws apply to your marketing campaign will depend on what country or countries you are targeting and/or collecting information from. As a general rule, marketers should:

- Think carefully about countries that require opt-ins (as opposed to opt-outs) and begin developing user lists for these countries as early as possible to optimize your marketing efforts. If you do not start early, you may never get your list to critical mass.
- Clearly and accurately label both the sender and the subject line of the email as well as provide a mechanism (e.g., unsubscribe link) for users to opt-out of receiving emails from the email sender.
- Ensure that any third party lists which you purchase or rent for marketing activities include the necessary permissions to collect and share such user email addresses.
- Scrub any third-party list against your unsubscribe lists to ensure that you do not send emails to users who have already opted out of receiving marketing emails from you.
- Strive to tailor global campaigns in such a way that allows you to leverage the benefits of email messaging in the more liberal environments, but be nimble enough to adhere to more rigid environments when needed.

Strive to tailor global campaigns in such a way that allows you to leverage the benefits of email messaging in the more liberal environments, but be nimble enough to adhere to more rigid environments when needed.

Mobile marketing

Direct messaging by way of mobile phone is quickly becoming a favored strategy to reach users in many markets. (Online advertising viewed on mobile browsers or email received on a mobile device is governed by applicable regulations referenced above.) However, because of its recent development and growth, very few jurisdictions have enacted regulations that restrict companies' use of direct marketing through SMS text messages. There are, however, some notable examples of SMS marketing restrictions:

- **US.** In the US, mobile marketing is governed by the CAN-SPAM Act of 2006 and the Telephone Consumer Protection Act (TCPA), in which advertisers may only send direct marketing texts to those mobile phone users who have given prior consent (opt-in) to receive such messages.

- **UK.** In the United Kingdom, direct marketing SMS text messages are subject to the same restrictions as direct marketing emails. This means that advertisers may only send direct marketing texts to those mobile phone users who have given prior consent (opt-in) to receive such messages. Additionally, the sender of such texts must clearly identify themselves in any messages.
- **India.** In India, recent telemarketing regulations resulted in an increase in the number of direct marketing text messages that mobile phone customers were receiving. In response, telecommunications regulators enacted a rule that limits mobile phone users to a maximum 100 text messages per day and limits the time of day that commercial email marketers can send commercial texts, thus greatly limiting the value of mobile marketing in India. It remains to be seen whether this regulation will survive since, on its face, it not only limits SMS marketing, but also greatly restricts the utility of SMS messaging overall. Further, India has established a “do not disturb” registry that marketers must comply with or face fines.

Key takeaways for marketers

Although regulation of mobile marketing is currently not widespread around the globe, the increase in the use of mobile marketing will undoubtedly attract new regulation. It seems likely that new regulation in this area will be based on, or analogous to, regulation of email and telemarketing. Mobile marketing programs should therefore consider implementing practices that would be acceptable for email marketing and telemarketing activities in the country in which the mobile marketing program is conducted. While not fail-safe, such a policy would both reduce the impetus for new and more onerous regulation and also position the mobile marketer for later compliance.

Telemarketing

Telemarketing, as with email marketing, is governed by a number of different regulatory schemes. The two most common of these schemes are opt-out schemes, wherein customers may request to be removed from calling lists used by advertisers, and opt-in schemes, in which marketing calls can only be made to those users who have given their prior consent to receive such calls. These regulations apply to both business and home phone numbers:

- **US.** In the US, telemarketing is governed by two primary regulations. First, the FTC maintains the National Do Not Call Registry. Telemarketers are prohibited from calling those telephone customers who have placed their phone number with the Registry. Second, the FCC places restrictions on the way in which telemarketers conduct their business, prohibiting the use of automated dialers and pre-recorded messages and limiting the timeframe for telemarketing calls to between 8 a.m. and 9 p.m.
- **UK.** The United Kingdom has adopted an opt-out scheme for the regulation of telemarketing similar to that of the United States. Telemarketers are prohibited from calling telephone customers who have registered their phone number with the Telephone Preference System, the national opt-out registry. Additionally, the use of automated calling systems is prohibited in all situations except where the recipient of the call has given prior express consent to receive calls made using such systems.
- **Australia.** Australia has also adopted an opt-out system with the passing of the Do Not Call Register Act of 2006. Unlike the US and UK models, however, no restriction is placed on the use of automated dialing systems.
- **India.** India has recently adopted a regulation that implements an opt-out scheme for telemarketing. Under the Indian system, telephone customers can register their phone numbers with a national customer preference list, allowing the customer to opt out of receiving telemarketing calls from specific commercial sectors. Additionally, the Indian system requires telephone service providers to maintain their own preference lists as well. All telemarketers

must register with, and receive certification from, the Telecom Regulatory Authority of India (TRAI) prior to making any telemarketing calls.

- **EU (Germany and France).** Since there is no specific EU directive on the topic, EU countries have developed their own regulatory frameworks to address telemarketing activities. In particular, Germany and France have each adopted restrictive opt-in regulatory schemes. Under German and French law, telemarketers may only make calls to telephone customers who have given prior consent to receive such calls.
- **China.** China has yet to adopt any regulations that govern telemarketing broadly. The country has, however, enacted industry-specific regulations that target telemarketing regarding specific products, such as insurance.

Key takeaways for marketers

Any telemarketing venture in a new country requires awareness of the type of regulatory scheme in place for that country. Regulations and restrictions to keep in mind include:

- Do-not-call-registries—If a national do-not-call registry has been put in place, the company must be certain to keep its call-list up to date with the registry, so as to avoid any type of sanctions or fines that might be imposed by telecommunications regulators.
- Opt-in systems—If an opt-in system is in place, then the company must be sure to consistently update its call lists to reflect telephone customers' requests to be removed.
- Time of day restrictions—Regardless of the regulatory scheme in place, be aware of restrictions on the time of day in which telemarketing calls are received by the user.
- Automated dialing—Unless a campaign targets a jurisdiction that does not restrict their use, automated dialing and calling systems should be avoided except in very limited circumstances.

If an opt-in system is in place, then the company must be sure to consistently update its call lists to reflect telephone customers' requests to be removed.

Laws and regulations applicable to content development and messaging

Although the above discussion has focused on the regulations that govern the technological methods of advertising chosen by a company, more general regulations regarding the content of advertisements must always be considered, regardless of the form the advertisement takes. For example, advertisements around the world, almost without exception, must not mislead or deceive users as to the nature, or source of, goods. Additionally, certain jurisdictions, such as India and China, has restrictions on the content of advertisements and on the nature of goods that can be advertised.

Comparative advertising. Comparative advertising is often regulated, either directly or via a country's interpretation of trademark rights. When an advertiser compares its goods with those of a competitor, that advertiser must be sure that the comparison does not violate any restriction on comparative advertising or the trademark rights of the competitor. Although many countries do not explicitly regulate comparative advertising, nearly every nation has placed some restrictions on advertising that have the effect of limiting those comparisons that are permissible through a combination of trademark, adverting and consumer protection laws.

In the following key jurisdictions, we find that comparative advertising (regardless of industry) is treated as follows:

- **United States, Australia, and India.** The United States, Australia, and India have no laws that specifically regulate the use of comparative advertisements, but instead rely upon a combination of truth-in-advertising regulations and trademark law to determine when a comparative advertisement is permissible. In general, the comparison must be factually accurate and must not use the competitor's trademark in such a way as to cause confusion as to source or sponsorship of the advertiser's products.
- **United Kingdom, France and Germany.** In the United Kingdom, France and Germany, regulations have been enacted that directly govern the use of comparative advertisements by restricting them to comparisons between products with a similar use or purpose and prohibiting misleading comparisons. Further, any comparisons made must be objective comparisons between material features of the goods or services. The law on comparative advertising has been harmonized throughout the EU by the EU Comparative Advertising Directive. If a comparative advertisement does not fall within the rules set out by the Comparative Advertising Directive, it will expose the advertiser to liability for trademark infringement. It may also be able to obtain redress through an action for trade libel, malicious falsehood, copyright infringement and passing off.
- **China.** In China, the use of comparative advertising is effectively prohibited by the Unfair Competition Law that restricts advertisements that belittle the goods of competitors. In fact, as the law is written and case law is applied, it would be difficult to try to utilize comparative advertising in China without running afoul of the law.

Key takeaways for marketers

According to TechTarget's 2011 Media Consumption Report on a survey of more than 4,000 information technology (IT) professionals worldwide, comparative content is one of the most sought after types of content IT professionals utilize to educate themselves on technology solutions. The majority of respondents indicated a desire for comparative content and this need is heightened when buyers are narrowing their potential purchase short-lists.

In light of this demand and the varying laws applied to comparative advertising, advertisers should not dismiss comparative content in the EU, but rather look for easily approachable content types like sponsorships of independent editorial content, analyst white papers, or third party test labs that might be allowable under the rules, such as the one that can be seen here. If you come to market with competitive content that complies with regulations, you could have a competitive advantage. Finally, when a US team is developing comparative advertising pieces that could potentially be used outside the US, it would be wise to review the regulations of your targeted countries before using outside the US.

Advertisers should not dismiss comparative content in the EU, but rather look for easily approachable content types like sponsorships of independent editorial content, analyst white papers, or third party test labs.

Emerging markets

Although established markets have put in place numerous regulations governing advertising and the many mediums through which it might be delivered, for the most part, emerging markets have yet to address the subject. In these markets, advertisers may determine the fashion in which they market goods at their own discretion in line with the company's overall brand development objectives. As these markets grow, however, increases in the number of advertisers targeting them will spur the creation of regulations similar to those already in place in established markets. For this reason, companies entering these markets would be best served by launching advertising campaigns that are tailored to withstand scrutiny under the regulatory regimes of markets in which they are already advertising

Final takeaways for marketers

Your next steps should be to ensure that your team is up to speed on the regulations that apply to the marketing campaigns you are running or plan to run in the future. This includes working with your legal team and third party partners to drive consistent compliance moving forward.

To aid you in this process, it is advisable to put processes in place to both maintain awareness of regulations that impact online marketing and ensure that their online marketing campaigns are operated in line with current best practices within the industry. Although not every online marketing campaign must be designed to comply with the most restrictive laws, **you should identify your strategic priorities** so that you can design campaigns that are compliant with the relevant laws in the targeted jurisdictions.

Practical questions to consider as you implement these strategic priorities:

- What **media vehicles** will be used to execute the campaign and what **compliance issues** apply to these vehicles?
- What **data** will be collected in connection with these activities, and what will be done with the data?
- In what **countries/states** will the collection and processing of the data occur?
- How will the data be **stored** and **secured** once collected?
- What is the most efficient policy to adopt to balance **global compliance** against **maximum utilization** of available data?

Glossary of terms

CAN-SPAM Act of 2006 (US)
The Controlling the Assault of Non-Solicited Pornography and Marketing Act is legislation written to regulate the sending of direct marketing emails in the United States. The Act requires that companies engaging in email marketing must not send emails to consumers that opt out from receiving advertisements. Companies sending emails for marketing purposes under the Act must ensure that all information in the email header and subject line are correct. Additionally, the Act requires that all marketing emails contain an address at which the recipient may send a request to opt out of receiving future emails, and that the sender honor such requests. Finally, all emails containing sexually explicit content must be labeled as such.

Data Protection Directive (EU)
EU Data Protection Directive (also known as Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. Directive 95/46/EC encompasses all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence. The Directive is based on the 1980 OECD "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data."

Directive 2006/114/EC/ Comparative Advertising Directive (EU)
Directive 2006/114/EC is an EU directive requiring member nations to adopt laws regulating the use of misleading and comparative advertising. Member nations are required to adopt laws that prohibit all misleading advertising. Comparative advertising is permissible under the directive, but the comparisons made must not be misleading, must be objective, and must be made between similar goods and features.

Directive on Privacy and Electronic Communications Regulations (UK)
The Privacy and Electronic Communications Regulations (PERC) is legislation implementing the E-Privacy Directive (EU). PECR regulations restrict the processing and sharing of personal traffic data and location data and provide for access to users' personal data in the interest of national security. The information commissioner has the power to audit the measures taken by a provider of public electronic communications services to comply with personal data breach notification and recording requirements.

Do Not Call Register Act of 2006 (Australia)
The Do Not Call Registry Act of 2006 is Australian federal legislation that created Australia's Do Not Call Register, an opt-out telephone list. Telephone service subscribers are eligible to record their telephone number on the list so long as the subscriber's number is both Australian and used primarily for domestic or private purposes. Certain types of organizations, such as governmental agencies, religious organizations, charitable groups and educational institutions are exempt from the prohibition on calling registered telephone numbers.

Do Not Call Registry (US)
The "do not call" registry is a list of phone numbers in the United States that telemarketers are prohibited from calling in most circumstances. The list is maintained by the National Do Not Call Registry of the Federal Trade Commission (FTC), and consumers can contact the agency to have their numbers registered. Organizations are prohibited from making calls to sell goods or services to any numbers listed, and are subject to substantial fines if they fail to comply.

E-Privacy Directive (EU)
E-Privacy Directive, formally known as Directive 2002/58 on Privacy and Electronic Communications, is an EU directive on data protection and privacy. The Directive requires member nations to adopt laws mandating that telecommunications providers ensure the confidentiality of all electronic communications and maintain the privacy of all traffic data. Additionally, the directive prohibits sending unsolicited electronic communications by means of email, fax and automated calling machine to anyone who has not given prior consent to receive such communications.

EU-US Safe Harbor framework
Safe Harbor is the name of a policy agreement established between the United States Department of Commerce and the European Union (E.U.) in November 2000 to regulate the way that U.S. companies export and handle the personal data (such as names and addresses) of European citizens. The agreement is a policy compromise set up in response to a European directive that differed from traditional business procedures for U.S. companies dealing with the E.U. In 1998, the E.U. established the European Commission Directive on Data Protection, which prohibited data transfer to non-European countries that did not adhere to stringent criteria. In effect, because the guidelines were very strict, they made it illegal to transfer most citizens' personal data outside of Europe.

Safe Harbor stipulations require that: companies collecting personal data must inform people that the data is being gathered, and tell them what will be done with it; they must obtain permission to pass on the information to a third party; they must allow people access to the data gathered; data integrity and security must be assured; and a means of enforcing compliance must be guaranteed.

European Economic Area
The European Economic Area (EEA) came into being on January 1, 1994, after the Agreement on the European Economic Area entered into force. The EEA unites the three member nations of the European Free Trade Agreement (EFTA)—Iceland, Liechtenstein and Norway—and the twenty-seven member nations of the European Union into a single market. The members of the EFTA are obliged to adopt all EU legislation relating to that single market.

Federal Trade Commission Act (US)
The Federal Trade Commission Act is the legislation that created the Federal Trade Commission (FTC) in 1914. The Act tasks the FTC with the creation and enforcement of rules aimed at curbing unfair trade practices.

Massachusetts information security regulations (US)
The Massachusetts Information Security Regulations took effect on March 1, 2010. These regulations set forth minimum standards in the care to be taken when processing the personal information of any resident of the Commonwealth of Massachusetts. Any company processing said information must establish risk-based information security program that contains specific safeguards mandated by the regulation, including safeguards regarding the selection of data storage facilities.

“Personally Identifiable Information” or PII
Personally identifiable information (PII) is any data about an individual that could potentially identify that person, such as a name, fingerprints or other biometric data, email address, street address, telephone number or social security number. A subset of PII is PIFI (personally identifiable financial information).

Spam Act of 2003 (Australia)
The Spam Act of 2003 is Australian federal legislation that was enacted on December 12, 2003. The Act aims to curb the use of direct marketing by email and other electronic communications. Under the

Act, marketing emails and messages can only be sent to persons who have given prior consent to receive such emails and messages. Commercial electronic messages must also include information about the individual or organization that authored the message and contain a function enabling recipients to unsubscribe from receiving future messages.

Telephone Consumer Protection Act or TCPA (US)
The Telephone Consumer Protection Act is legislation written to regulate the use of telemarketing in the United States by amending the Communications Act of 1934. The Act limits the time of day that telemarketing calls can be made to between 8 a.m. and 9 p.m. local time. The Act also requires that solicitors maintain “Do Not Call” lists that must be honored for a period of five years, and limits the situations in which a solicitor may use automated dialers and prerecorded calls.

Telephone Preference System (UK)
The Telephone Preference Service is an opt-out telephone list in UK that has been active since May of 1999. The list currently derives its statutory authority from the Privacy and Electronic Communications Regulations of 2003. In 2004, the Regulations were amended to allow corporate telephone subscribers to register with the list. Telemarketing calls cannot be made to numbers registered with the Service unless the owner of that number has previously notified the caller that they do not object to receiving such calls.

Uniform Commercial Code
The Uniform Commercial Code (UCC) is a uniform act first published in 1952 with the goal of harmonizing state laws governing commercial transactions throughout the United States. The UCC is concerned primarily with transactions involving personal property as opposed to real property, and has been adopted throughout the United States.

About the author

Gina Perini is Managing Counsel at GTC Law Group LLP (www.gtclawgroup.com) where she heads up the New Media practice group, an interdisciplinary practice combining strategic trademark, privacy and internet law to support businesses in the digital economy. Gina advises clients in global intellectual property and business matters in the technology, telecommunications, internet, new media, advertising and consumer product sectors. She has extensive experience in international privacy and data protection compliance, cross-border outsourcing transactions, technology and licensing transactions, and a wide range of copyright and trademark matters.

GTC Law Group LLP specializes in IP Strategy, Mergers & Acquisitions, and Business & Technology Transactions for IP-centric companies and institutions worldwide.

About TechTarget

TechTarget (NASDAQ: TTGT) is the online intersection of serious technology buyers, targeted technical content and technology providers worldwide. Our extensive network of online and social media, powered by TechTarget's Activity Intelligence™ platform, redefines how technology marketers view and engage technology buyers based on their active projects, specific technical priorities and business needs. With more than 100 technology-specific websites and a wide selection of custom advertising, branding, and lead generation solutions, TechTarget delivers unparalleled reach and innovative opportunities to drive technology marketing success around the world.

TechTarget has offices in Atlanta, Beijing, Boston, Cincinnati, London, Mumbai, San Francisco, Singapore and Sydney.

To learn how you can engage with serious technology buyers worldwide, visit techtarget.com and follow us @TechTarget.