WAHAB & MEDENICA LLC
125 MAIDEN LANE, SUITE 208, NEW YORK, NY 10038 | 212-785-0070 | www.WRLAWFIRM.com

Top Ten Laws any Online Operation Should Know. A Quick Guide.

By Kaiser Wahab and Lauren Mack

Below is a top ten pocket guide for the top ten laws any operation (social, e-commerce, IP/UGC driven, etc.) needs to be familiar with now and for the foreseeable future. Having this at the ready won't necessarily make you smarter, but it will certainly make you more prepared (and should you want to delve further into any one of them, there is much, much more info on the net).

1) Anti-Counterfeiting Trade Agreement (ACTA)

ACTA is an international agreement to create uniform standards for intellectual property (IP) enforcement. It requires participating countries to comply with civil and criminal IP enforcement standards and remedies, quickly and effectively enforce IP laws online, provide protection against the circumvention of technological measures, create specialized bodies to enforce IP rights, give IP enforcement power to border authorities, and cooperate with the other countries in the fight against IP infringement. Many of the provisions regarding the Internet resemble the United State's DMCA (see #8 below), but they do not require signing countries to adopt the limitations on liability included in United States copyright law, such as fair use or the complete immunity from monetary damages for service providers available under the DMCA.

For More Info: http://www.ustr.gov/acta

2) Anticybersquatting Consumer Protection Act (ACPA)

ACPA is a federal law that creates a civil cause of action against cybersquatters. Cybersquatters register domain names that contain or are confusingly similar to another's trademark for the sole purpose of selling it to trademark owner. Uses that are using the trademark to identify the owner's product or service, such as fan or gripe sites, would not be subject to ACPA because liability is based on the bad faith intent to profit from the domain name. A successful trademark holder can choose to either have the domain name cancelled or transferred to the mark holder, and in some cases may also be able to obtain damages.

For More Info: http://www.chillingeffects.org/acpa/faq.cgi

3) Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM)

The CAN-SPAM Act is a federal law that regulates unsolicited commercial email. It prohibits senders of commercial emails meant as advertising or promotion from including false or misleading information or using deceptive subject headings. It also requires the sender of a commercial email to disclose that the email is an advertisement, use an accurate return email address, include an opt-out option that is honored promptly, and provide a physical address.

WAHAB & MEDENICA LLC

For More Info: http://business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business

4) Communications Assistance for Law Enforcement Act (CALEA)

CALEA is a federal law that requires telecommunications carriers to choose their equipment and design their services to allow the government to easily conduct electronic surveillance in real time without the user knowing that the communication is being monitored. All providers of digital telephone service, broadband Internet access, and VoIP services must comply with CALEA.

For More Info: http://www.fcc.gov/calea/

5) Communications Decency Act of 1996 (CDA)

The CDA is a federal law that includes one of the most powerful shields from liability for Internet intermediaries. §230 of the CDA provides immunity from liability for any provider or operator of an interactive computer service that publishes information provided by others. To use §230 as a shield from liability, the provider of the interactive computer service may delete the information provided by a user, but cannot contribute to the content submitted by the user, including through selective editing. This section has so far provided complete immunity from defamation, negligent misrepresentation, infliction of emotional distress, and other claims to a broad range of interactive computer services, but it also often leaves the harmed party without a remedy. It does not apply to federal criminal law, intellectual property law, or electronic communications privacy law.

For More Info: https://www.eff.org/issues/bloggers/legal/liability/230

6) California Online Privacy Protection Act of 2003 (OPPA)

OPPA is a California state law that requires any individual or entity that collects personally identifiable information (PII) from California residents through the Internet to have a privacy policy that is plainly visible. Although it is a state law, it affects any website or mobile application available in the United States that collects PII from its users, as the likelihood of a California resident using any given website or mobile application is very high. PII is defined in the Act as any information that allows an individual to be contacted, including a first and last name, physical address, email address, phone number, or social security number. The privacy policy must at the very least include what type of information is gathered by the website, the kinds of third parties that information may be shared with, how the user can review and make changes to their stored information if the ability to do so is offered, how users will be notified of any material changes to the policy, and the policy's effective date.

For More Info: http://oag.ca.gov/privacy/COPPA

7) Children's Online Privacy Protection Act (COPPA)

COPPA is a federal law enforced by the Federal Trade Commission that bars commercial websites or online services directed at children under the age of thirteen, or that have actual knowledge that children under thirteen are providing information online, from collecting personal information from someone under thirteen years old without verified parental consent. Verified parental consent can be obtained through many ways, including by verifying a credit card number, receiving an email with a digital signature, or accepting a phone call from the

WAHAB & MEDENICA LLC

parent. If a website does have a process for obtaining parental consent, there must be a privacy notice detailing what information is being collected, how it is being used, whether it is being disclosed to third parties, and other relevant information listed in the Act.

For More Info: http://www.coppa.org/

8) Digital Millennium Copyright Act (DMCA)

The DMCA is a federal law that creates a "safe harbor" for online service providers from being held monetarily liable for their users' copyright infringement. To have the protection of the safe harbor provision, the service provider cannot have actual knowledge of infringement, cannot receive a direct economic benefit when it has the right and ability to control the activity, and must quickly remove or disable access to infringing material once it has actual knowledge or notice of the infringing content. The service provider must have a system in place to process takedown notices as detailed in the Act, and the courts have added that it may not induce its users to commit copyright infringement or hold itself out as a service meant to be used for copyright infringement.

For More Info: http://brainz.org/dmca-takedown-101/

9) Electronic Communications Privacy Act (ECPA)

ECPA is a federal law that includes the Wiretap Act and the Stored Communications Act. The Wiretap Act extends the privacy protections given to telephone calls to electronic communications by making it illegal for anyone, including the government, to intentionally intercept the contents of an electronic communication using a device without a warrant or consent from one of the parties. Service providers that must intercept electronic communications in order to provide their services are exempted.

The Stored Communications Act (SCA) makes it illegal to intentionally access stored electronic communications and for the provider of an electronic communication service to disclose that information without the user's consent, disclosure being necessary to providing the service, or an emergency situation where the provider believes in good faith harm could be avoided by disclosure to the government. Under the SCA, the government must have a search warrant to access unopened emails that have been stored for 180 days or less, but access to communications older than 180 days only requires a subpoena or prior notice (which may be delayed) and a court order based on "specific and articulable facts," which is a lower standard than the probable cause needed for a search warrant. Whether accessing opened emails that have been stored for 180 days or less requires a search warrant is uncertain.

For More Info: http://www.cybertelecom.org/security/ecpa.htm

10) Uniform Dispute Resolution Policy (UDRP)

The UDRP is a process created by the Internet Corporation for Assigned Names and Numbers (ICANN) to resolve disputes over domain names. It is a lot like ACPA in that the plaintiff must show that the domain name is the same or confusingly similar to it's trademark, that the defendant has no rights or legitimate interests in the name, and that the domain name is being used in bad faith. UDRP proceedings are generally preferred by plaintiffs because they are cheaper, faster, and pro-plaintiff, but the only remedies available are cancellation or transfer of the domain name.

For More Info: http://www.icann.org/en/help/dndr/udrp/policy