Internet Law Social Media and Privacy

1. Internet Law
2. Copyrights in Digital Information
3. Social Media
4. Online Defamation
5. Privacy

Unsolicited e-mails SPAM

1. State Regulations;

Many state laws that regulate SPAM require the senders of e-mail ads to instruct the recipients on how they can “opt out”.

2. Federal Regulations; (2003)

“ Controlling the Assault of Non-Solicited Pornography and Marketing Act (can-spam).

3. U.S. Safe Web Act;

After the CAN-SPAM Act of 2003 prohibited false and deceptive e-mails originating in the U.S., spamming from servers located in other nations increased. Congress enacted the “Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Boarders Act”.

The Safe Web Act also provides a “safe harbor” for Internet Service Providers (ISPs)—that is, it gave them immunity from liability for supplying information to the Federal Trade Commission (FTC) concerning possible unfair or deceptive conduct in foreign jurisdictions.

Domain Names

STRUCTURE OF DOMAIN NAMES

Every domain name ends with a generic top-level domain (TLD), which is the part of the name to the right of the period that often indicates the type of entity that operates the site. e.g.. .com is an abbreviation for commercial, and .edu is short for education.

The second-level domain (SLD)--the part of the name to the left of the period—is chosen by the business entity or individual registering the domain name.

DISTRIBUTION SYSTEM

The Internet Corporation for Assigned Names and Numbers (ICANN), oversees the distribution of domain names and operates an online arbitration system.

In 2012, ICANN started selling new generic top-level domain names (gTLDs) for an addition price of $185,000 plus $25,000 annually. gtlds can take on any form such as .aol, .bmw, .gmail or .Youtube.

Cybersquatting

One of the goals for the new gTld system was to alleviate the problem of cybersquatting.

Cybersquatting occurs when a person registers a domain name that is the same as, or similar to, the trademark of another and then offers to sell the domain name back to the trademark owner.

ANTICYBERSQUATTING LEGISLATION

Because cybersquatting had led to so much litigation, Congress enacted the Anticybersquatting Consumer Protection Act (ACPA), which amended the Lanham Act. The ACPA makes cybersquatting illegal when both of the following are true:

1. The name is identical or confusingly similar to the trademark of another.
2. The one registering, trafficking in, or using the domain name has a "bad faith intent" to profit from that trademark.

TYPOSQUATTING

Typosquatting is when a person register a domain name that is a misspelling of a popular brand or product.

APPLICABILITY AND SANCTIONS OF THE ACPA

The ACPA applies to all domain name registrations of trademarks. Successful plaintiffs in suits brought under the act can collect actual damages and profits, or they can elect to receive statutory damages ranging from $1,000 to $100,000.

COPYRIGHTS IN DIGITAL INFORMATION

1. In 1998 Congress passed legislation to protect copyright holders, The Digital Millennium Copyright Act (DMCA). The DMCA gave significant protection to owners of copyrights in digital information. Among other things, the act established civil and criminal penalties for anyone who circumvents encryption software or other technological antipiracy protection.

2. The DMCA provides for exceptions to fit the needs of libraries, scientists, universities and others. In general, the law does not restrict the "fair use" of circumvention methods for educational and other noncommercial purposes.

3. The DMCA also limits the liability of ISPs. Under the act, an ISP is not liable for copyright infringement by it's customers unless the ISP is aware of the subscribers violation.

MP3 and File-Sharing

Soon after the Internet became popular, programmers created new software to compress large data files, particularly those associated with music.

File sharing is accomplished through peer-to-peer (P2p) networking. Rather than going through a central Web server, P2P networking uses numerous PCs that are connected to the internet, individuals on the same network can access files stored on one another's PCs through a "distribution network".

When file-sharing is used to download others' stored music files, copyright issues arise.

DVDs and File sharing

File sharing also creates problems for the motion picture industry. Numerous Web sites offer software that facilitates the illegal copying of movies.

Social media

- Social networking sites, such as Facebook, Google+, MySpace, Linkedin, Pinterest and Tumblr have become ubiquitous.
- The emergence of these sites has created a number of legal and ethical issues for businesses. Social media posts now are routinely included in discovery in litigation.
- Tweets and other social media posts can also be used to reduce damage awards.
- Law enforcement uses social media to detect and prosecute criminals.
- Federal regulators also use social media posts in their investigations into illegal activities.
- Employees who use social media in a way that violates their employer's stated policies, can be terminated.

The Electronic Communications Privacy Act (ECPA)

1.Part of the ECPA is known as the Stored Communications Act (SCA).The SCA prohibits intentional and unauthorized access to stored electronic communications and set forth criminal and civil sanctions for violators.

2.Protection of Social media Passwords. Employers and Schools have sometimes asked for an individuals password to their social media accounts. Some states have enacted legislation to protect individuals from having to disclose their social media passwords. The federal government is also considering legislation that would prevent employers or schools from demanding passwords to social media accounts.

3.Many companies have implemented their own Company-wide Social Media Networks to guard trade secrets, maximize production of their employees and reduce the amount of time dealing with e-mails.

Online Defamation

- Cyber Torts are torts that arise from online conduct. One of the prevalent cyber torts is online defamation. Because the internet enables individuals to communicate with large numbers of people simultaneously, online defamation has become a problem in today's legal environment.
- An initial issue raised by online defamation is simply discovering who is committing it. Online forums allow anyone to complain about a company or firm that they dislike while remaining anonymous. Therefore, a threshold barrier to anyone who seeks to bring an action for online defamation is discovering the identity of the person who posted the defamatory message.
- Consequently businesses and individuals are increasingly bring lawsuits against "John Does", then, using the authority of the courts, they can obtain from the ISP's the identity of the persons responsible for the defamatory messages.

Privacy

Facebook, Google, and Yahoo have all been accused of violating users' privacy rights.

To maintain a suit for the invasion of privacy, a person must have a reasonable expectation of privacy in the particular situation.

People clearly have a reasonable expectation of privacy when dealing with their personal banking or credit card accounts, or that a company will follow their own privacy policies. But it is probably not reasonable to expect privacy in statements made on Twitter.

Data Collection and Cookies

Cookies are invisible files that are collected to track a user's Web browsing activities.

Cookies provide detailed information to marketers about an individual's behavior and preferences, which is used to personalize online services.

The FTC investigates consumer complaints of privacy violations. The FTC has forced many companies to enter into a consent decree that gives the FTC broad power to review their privacy and data practices.

The Consumer Privacy Bill of Rights

1. Individual Control—Consumers have the right to exercise control over what personal data organizations collect from them and how they use it.
2. Transparency—Consumers have the right to easily understandable information about privacy and security practices.
3. Respect for Context– Consumers have the right to expect that an organization will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
4. Security– Consumers have the right to secure and responsible handling of personal data.
5. Access and Accuracy– Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
6. Focus Collection– Consumers have the right to reasonable limits on the data that companies collect and retain.
7. Accountability– Consumers have the right to have personal data handled by companies with appropriate measures in place to assure that they adhere to the Privacy Bill of Rights.