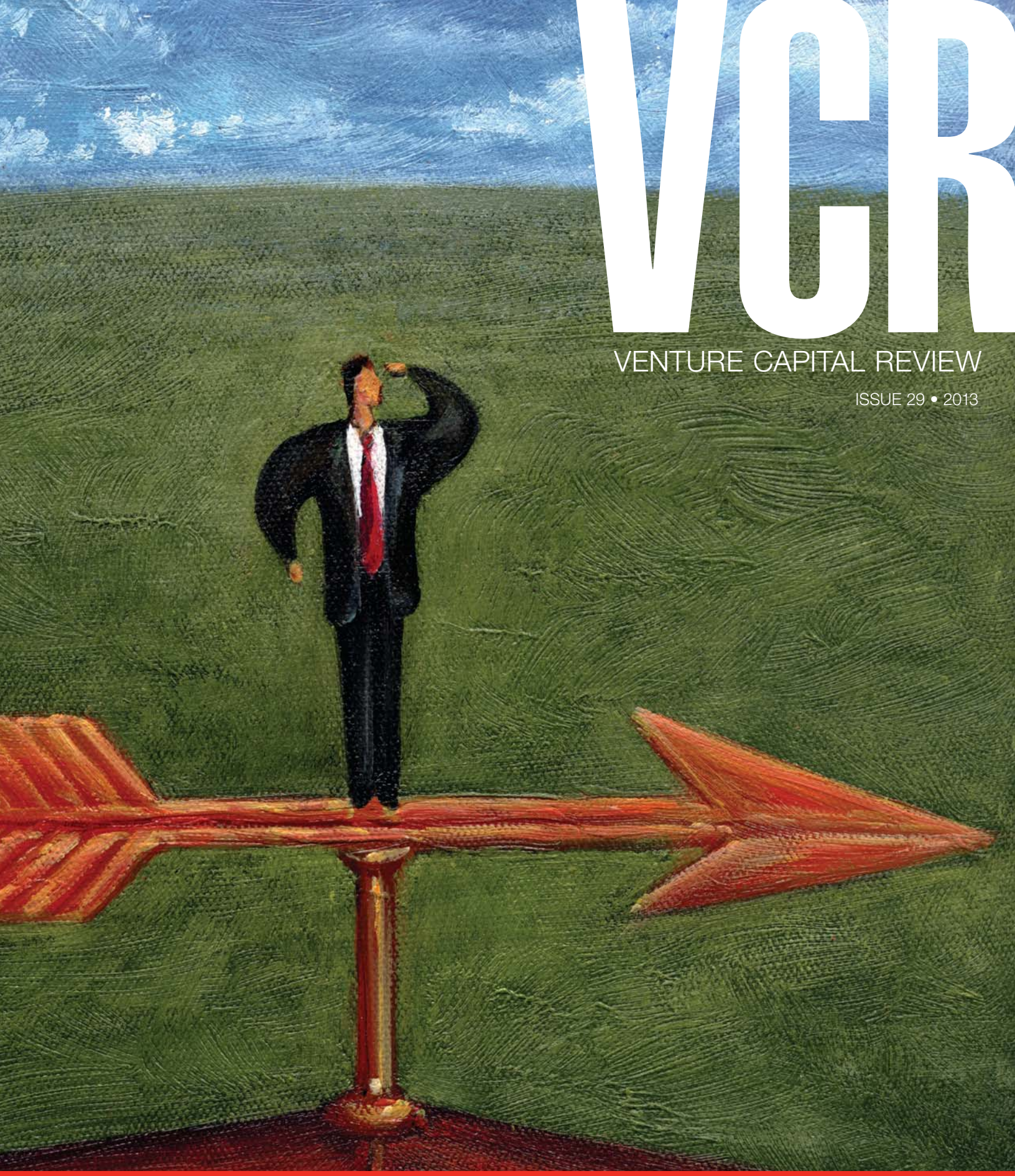


VCR

VENTURE CAPITAL REVIEW

ISSUE 29 • 2013

PRODUCED BY THE NATIONAL VENTURE CAPITAL ASSOCIATION AND ERNST & YOUNG LLP

National Venture Capital Association (NVCA)

As the voice of the U.S. venture capital community, the National Venture Capital Association (NVCA) empowers its members and the entrepreneurs they fund by advocating for policies that encourage innovation and reward long-term investment. As the venture community's preeminent trade association, NVCA serves as the definitive resource for venture capital data and unites its 400 plus members through a full range of professional services. Learn more at www.nvca.org.

National Venture Capital Association

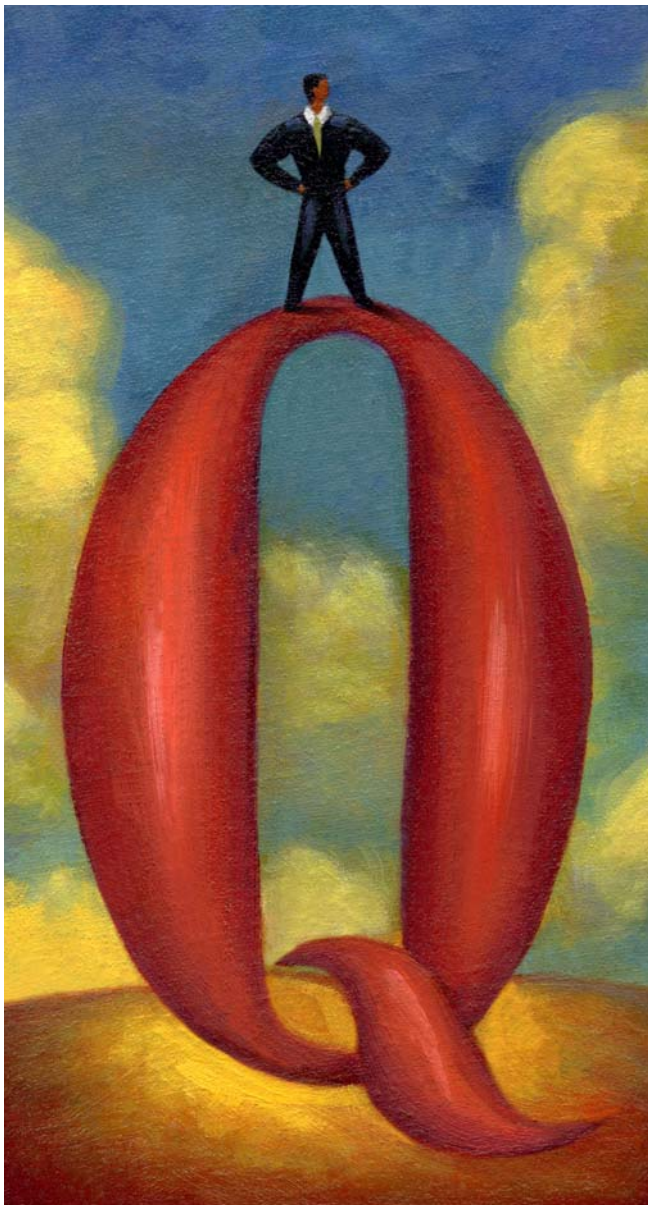
1655 Fort Myer Drive
Suite 850
Arlington, VA 22209

Phone: 703.524.2549
Fax: 703.524.3940
Web site: www.nvca.org

Proskauer

Antonio Who? Investing in New Media and Social Media — When Legal Issues Become Business Issues

Kristen Mathews and Paresh Trivedi, Proskauer Rose, LLP



New media and social media start-ups often provide interesting and attractive investment opportunities. When examining investment opportunities in this space — in addition to conducting routine analyses of a company's products and services, potential to generate income and profits, competiveness, prospects for growth and potential exit strategy — investors should also understand the unique legal and regulatory issues facing such companies, as these issues can significantly impact a company's value.

Appropriate protection and management of intellectual property rights and compliance with legal and regulatory requirements are as important to a company's present and future value and growth as the ingenuity of its products and services and the soundness of its business plan. The story of Antonio Meucci is just one example of how a good idea without appropriate attention to legal issues can lead to a start-up's failure. Meucci, an inventor and entrepreneur, developed the world's first device capable of electromagnetic voice transmission in 1856. Today, however, his name and the name of his start-up, the Telettrofono Company, are largely unknown because Meucci failed to adequately protect his intellectual property rights. This misstep opened the door for Alexander Graham Bell to obtain a patent for electromagnetic transmission of vocal sound in 1876 and attain recognition as the inventor of the telephone. As a result, Bell and his start-up went on to enjoy success, wealth, fame, and a place in history, while Meucci's start-up failed.

This article provides an overview of some of the intellectual property, legal, and regulatory issues that investors should consider when evaluating investment opportunities in new media and social media companies.

I. Intellectual Property Rights for Technology Assets

Securing rights in intellectual property is vital for new media and social media companies, given the relative ease of emulating competitors online and the fact that intellectual property often comprises the most valuable and important assets in new media and social media. In light of this, companies should utilize all means available to develop and protect a robust intellectual property portfolio. At a minimum, each company should register material eligible for trademark and copyright protection, and obtain strong patent rights to its inventions, if appropriate. Once intellectual property rights are acquired, the company should take proper action to preserve those rights against infringers. Failure to actively defend intellectual property rights may constitute acquiescence to the infringement and adversely affect a company's value and competitive advantage.

Companies must also secure full ownership to all intellectual property their employees and contractors produce through enforceable work-for-hire and intellectual property assignment agreements. Work-for-hire agreements formalize the concept that ownership of copyrights in works produced in the course of employment belong to the company, and not to the employee or contractor who creates the work. Intellectual property assignment agreements assign all right, title, and ownership in patents, trade secrets, copyrights, and other intellectual property rights from an employee or contractor to the company.

Without effective work-for-hire and intellectual property assignment agreements, a company may fail to secure ownership of valuable intellectual property assets, causing significant loss in the company's value and competitive advantage.

In addition, maintaining a strong online presence requires the registration and protection of domain names that identify and distinguish the enterprise and its online brand. When use of the Internet for commercial transactions began in the 1990s, few restrictions governed the registration of domain names. "Cybersquatters," who registered domain names containing trademark terms in order to sell them to the trademark owner, were prevalent. In 1999, the Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit organization charged with managing assigned domain names, implemented a uniform policy for resolving domain name disputes through mandatory arbitration. Around the same time, the U.S. Congress adopted the Anticybersquatting Consumer Protection Act (ACPA), which gave trademark owners new tools for combatting cybersquatting.[1] Since then, numerous top level domain names have been added to the system, increasing the burden of companies to protect their brands' use in domain names. New media companies should understand the limitations on using certain domain names, as well as the tools for protecting their own trade names.

---

1 The ACPA amends the Lanham Act, the centerpiece of trademark legislation, to provide that a person who registers, traffics in, or uses a domain name that is identical or confusingly similar to a protected mark or that is dilutive of a famous mark will be subject to civil liability if the person has a bad faith intent to profit from the mark. Anticybersquatting Consumer Protection Act of 1999, Pub. L. No. 106-113, 15 U.S.C. § 1125(d).

Another intellectual property issue facing new media companies arises if a company incorporates open source software when developing its own technology. Open source software, sometimes referred to as "free software," is software that is made available in source code form. This way, in contrast to proprietary or "closed code" software, the code can be read, modified, and redistributed by users. Using open source software to develop proprietary products may reduce the cost and time required to bring a product to market. However, if not used properly, open source software could result in a company being forced to disclose the "secret sauce" behind its product or being exposed to liability, thereby negatively impacting the company's competitiveness and value.

II. Safe Harbors for User-Generated Content

In addition to securing its own intellectual property, new media companies often engage in activities that may result in the infringement of intellectual property rights held by another party and subsequent exposure to liability. On a basic level, the duplication and online transfer of unauthorized copies has induced industry-wide shifts in fields dominated by owners of copyrighted works, such as books, music, and video content. The increased availability of copyrighted information online and the new mechanisms for electronically sharing copyrighted information have made it easier to infringe upon exclusive rights. For example, seemingly innocuous electronic actions, such as providing a hyperlink to third-party content, may expose the operator of a website to liability if the link offers access to unauthorized copies of a protected work.[2] At the same time, copyright owners find it more difficult to enforce their rights, because, among other challenges, it may be difficult to identify the offending party or parties. Content owners have responded with litigation against the operators of file-sharing sites, file-sharing technology distributors, and individual file-sharers. Such litigation, in parallel with legislation, continues to shape and refine the body of law dealing with potential liability for certain online actions that do not fit neatly into the legal framework existing before the digital age.

A. Digital Millennium Copyright Act

The interactive nature of social media means that online service providers no longer generate all of their own content. Rather, consumers use online platforms as a forum for sharing self-generated content with other consumers interested in similar content. Although providers typically hold the ultimate control over content — that is, they retain the discretion to monitor and remove undesirable content — the proliferation of user-generated content makes it highly burdensome, if not impracticable, to adequately review such content on a real-time basis. At the advent of social media, it was feasible that online service providers could bear responsibility for all content, including user-generated content, on their online platforms. That is, if a user posted infringing content in an online forum, the service provider could be held liable for copyright infringement. Such a policy would have necessarily limited the ability of new media companies to offer a forum for instant and open communication, due to the threat of crippling liability and the resources required to review content prior to posting. Rather than leaving it to the court system to address, policymakers addressed this issue in favor of encouraging free and open speech online.

---

2 See e.g. *Jones Day v. Blockshopper LLC d/b/a Blockshopper.com, et al.*, 2008 U.S. Dist. LEXIS 94442 (N.D. Ill. Nov. 13, 2008), the court found a possible basis for trademark infringement claims in hyperlinks on a real estate firm's website to biographies of its attorneys; *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007), the Ninth Circuit held that a search engine was not liable for direct infringement for in-line linking to plaintiff's photographs on third-party sites, but remanded the case to determine whether a search engine could be liable for contributory infringement; the parties settled. But see *Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012) where the court found that a video bookmarking site where users embedded and stored links to third-party videos was not likely liable for contributory infringement.

The Digital Millennium Copyright Act (DMCA) contains "safe harbor" provisions that immunize some online service providers, under certain circumstances, from liability for user-generated content that infringes a copyright and appears on their platforms.[3]

As a threshold matter, to be afforded the safe harbor, the content may not be generated, selected, or edited by the service provider. Next, online service providers must meet three key requirements in order to qualify for the safe harbor. First, the provider must register a designated agent to receive notifications of claimed infringement with the U.S. Copyright Office. Second, the provider must expeditiously block access to or take down infringing material upon notice of infringement. Third, the provider must adopt and reasonably implement a policy of terminating the accounts of repeat infringers. In addition to limiting liability of online service providers, the DMCA also improves the means for copyright owners to reach the user posting the infringing content, without substantially increasing the burden on service providers. In this way, the DMCA attempts to balance competing interests by creating a limited safe harbor that encourages online service providers to permit free speech, while protecting the rights of copyright owners.

B. Communications Decency Act

The capability to communicate online—immediately and over vast distances—to large numbers of people has countervailing positive and negative aspects, particularly in the context of free speech and defamation. This accessible method for instantaneous and far-reaching communication carries clear benefits in disseminating useful information. Yet, it compounds the damage of false, misleading, or defamatory information, and such damage is often irreparable. This dichotomy is well-reflected in legislative enactments regulating online activity, such as the Communications Decency Act (CDA).[4] Through the CDA, Congress sought to strike a balance between protecting free speech online and guarding against false and damaging speech.

At a basic level, the CDA contains a safe harbor provision that immunizes an innocent "middleman" who merely provided an online forum for speech. Specifically, Section 230(c)(1) of the CDA states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Section 230 has been liberally interpreted to offer broad immunity to interactive service providers, such as website or mobile app operators, from defamation and other tort-type claims based on content generated by third-party users.[5] However, the CDA safe harbor does not grant immunity for the speaker itself, whether that is a user of a social media platform or the service provider. In practice, this federal law eliminates one barrier for online service providers permitting consumer free speech on interactive internet platforms by limiting potential liability of the service provider for user-generated content.

III. Digital Privacy

A. Privacy Policies

Privacy law continues to evolve rapidly in an increasingly digital environment. The collection, storage, and use of personally identifiable information in electronic commerce and online advertising has roused controversy, forming the basis of numerous legal disputes under existing laws and spurring development of new laws to deal with changing circumstances.

---

3 17 U.S.C. §§ 512(a)-(e).

4 47 U.S.C. § 230.

5 See, e.g., *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997) (holding that Section 230(c)(1) confers immunity on service providers for both publisher and distributor liability with respect to tort-like claims).

In most respects, the United States lacks uniform privacy legislation. Rather, privacy laws in the United States stem from various sources and form a complex and varied legal "patchwork." Indeed, privacy law consists of common law principles rooted in federal and state constitutional provisions, federal and state statutes specific to subject matter like health and financial information, and communications privacy laws that limit access to communications by law enforcement and third parties. In addition, administrative agencies like the Federal Trade Commission (FTC) and other consumer protection agencies provide a regulatory overlay for privacy issues. Online service providers must take care to determine which laws govern and what compliance requires.

One requirement is that all online service providers must adopt, conspicuously post, and adhere to a privacy policy that, among other things, identifies what kinds of personally identifiable information will be collected and with whom the data will be shared. Although federal legislation does not currently require a general commercial website to disclose a privacy policy, California has enacted and enforced this requirement in the California Online Privacy Protection Act (OPPA). Importantly, this law reaches far beyond California firms and purports to apply to every website and online service that collects personally identifiable information from California residents.[6] The practical consequence is that this important piece of California legislation impacts commercial websites and online services across the globe. After a company adopts its privacy policy, the FTC requires that the firm adhere to that policy, or else risk an action for unfair and deceptive trade practices.[7] The FTC has brought a number of enforcement actions against online providers that breached privacy promises or otherwise failed to keep consumer data secure.[8]

Tailoring a privacy policy to fit the unique needs of each business is essential to shielding the firm from liability and preserving its value as a prospective target for future investment or acquisition.

Some start-ups fall into a trap with far-reaching consequences by approaching its privacy policy with a one-size-fits-all mentality that is far removed from the legal reality. A privacy policy drafted for a seemingly similar business cannot be copied and pasted without tailoring to a company's specific needs. There is no such thing as a boilerplate privacy policy, because every company collects, manages, shares, and uses data differently. Moreover, it is very difficult to remedy an inaccurate or inapplicable privacy policy, due to restrictions on making material adverse retroactive changes to privacy policies after they have been adopted and communicated to users, absent affirmative consent to such change by consumers. Therefore, in order to limit exposure to privacy-related liability, companies operating online businesses or services should take care to adopt and implement the correct privacy policy from the beginning.

B. Mobile Applications

Similar to more traditional online platforms, such as Internet portals and websites, privacy is a crucial consideration in developing and deploying mobile applications, or apps. Moreover, the unique features offered by mobile apps only enhance the importance of digital privacy. For example, many mobile apps have the powerful ability to identify the precise location of a user, a function known as geolocation. This ability to track geographic movement, and the accompanying ability to target advertising and content based on that data, requires permission from the user and caution by the party collecting data to mitigate privacy concerns.

---

6 California Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22575 et seq.

7 Section 5 of the Federal Trade Commission Act (FTC Act) prohibits unfair or deceptive trade practices. 15 U.S.C. § 45.

8 See, e.g., *In re Google, Inc.,* FTC File No. 1023136 (Settlement announced Mar. 30, 2011) (settling deceptive practices charges against Google relating to the rollout of the Google Buzz social network in 2010, including charges that Google violated the substantive requirements of the E.U. -U.S. Safe Harbor agreement); *In the Matter of Chitika, Inc.,* FTC File No. 1023087 (Mar. 14, 2011) (settling charges of deceptive practices with an online advertising company that gave consumers the opportunity to opt out of its tracking cookies, but limited the opt-out period to ten days).

Data collection through mobile apps occurs in various ways: requesting users to provide information, accessing information stored on the mobile device, or collecting information automatically during use of the app. In addition to collecting typical personally identifiable or sensitive information (such as name, contact information, financial information, or health information), mobile apps may also collect information uniquely associated with mobile device technology, such as hardware identifiers or location data. It is important to note that tracking users with unique persistent identifiers still implicates privacy issues, even without access to more traditional personal identifiers like name and contact information.

In general, online service providers are subject to the same privacy requirements when offering mobile apps as with more traditional online services. Given the unique issues presented by mobile app technology, the FTC and state regulators have prioritized enforcement related to mobile privacy. Moreover, based on agreements among California authorities and six owners of leading mobile app stores, app stores must now provide a mechanism for mobile app developers to disclose privacy policies and for users to report non-compliance with California privacy law. Like the far-reaching scope of OPPA for traditional online platforms, these requirements apply globally to any mobile app that may impact California residents. California can seek to enforce this law against any mobile app provider that fails to comply by posting a privacy policy for the app. In order to minimize the legal and financial liability and reputational harm that could occur as a result of a privacy breach, companies should consider privacy as a critical and ongoing issue when developing and distributing a mobile app.

C. Age-Related Concerns

Federal and state authorities have placed particular importance on enforcing laws protecting the privacy of children online. The Children's Online Privacy Protection Act (COPPA) impacts operators of websites or online services that are directed to children under thirteen, as well as providers that have actual knowledge that children under thirteen are providing personal information through the website or online service.[9] At a basic level, COPPA requires covered online services to provide notice of what information they collect and how they will use that information. With some exceptions, a provider must obtain verifiable parental consent before collecting any personal information from children. Online service providers must also provide parents with access to review and change both the collected information and the manner in which providers use the information. The FTC vigilantly enforces COPPA against operators of websites and online services who fail to comply with its requirements.[10] As a result, awareness of and compliance with age-related requirements should be key concerns for new media companies.

---

9 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

10 See, e.g., *FTC v. Xanga.com, Inc.,* No. 06-CIV-6853 (S.D.N.Y. settlement entered Sep. 12, 2006) (assessing a $1 million civil penalty against a social networking site that allowed the creation of accounts by individuals whose birth date information indicated an age under 13, without complying with COPPA parental notice and access requirements); *United States v. Industrious Kid, Inc. FTC File No.: 072-308* (assessing a $130,000 fine for, among other things, enabling children to create imbee accounts by submitting their first and last names, dates of birth, and other personal information prior to the provision of notice to parents or the receipt of their consent).

IV. Data Security

The proliferation of online communications and commerce has accelerated the creation of large databases containing many types of personal information, from contact and financial information to shopping preferences and browsing histories. These valuable databases of personal information are open to misuse, whether at the hands of the online service provider that compiles the information or a hacker that wrongfully accesses a database. This intrinsic risk has driven the adoption of laws aimed at protecting those repositories from unauthorized access and data theft and protecting the public from the harmful effects of such misuse.

Pursuant to the Federal Trade Commission Act, the FTC has employed two key theories to take action against companies that fail to maintain the security of consumer data. The first position is that failure to comply with published security promises is deceptive. The second is that failure to use reasonable means to secure data is an unfair trade practice. Recently, the FTC has brought actions for failure to adequately secure data, even in the absence of a specific promise in a privacy policy to maintain consumer data securely.[11] The FTC has also taken the position that the act of distributing technology that jeopardizes the security of personal consumer information may constitute an unfair or deceptive trade practice. Firms must take care to avoid the costs, both monetary and reputational, incurred as a result of problems with data security.

In addition, the Securities and Exchange Commission (SEC) has issued guidelines suggesting that public companies have an obligation to disclose cybersecurity risks and cyber incidents publicly.[12] The SEC guidelines suggest that companies should routinely disclose such information alongside preexisting disclosure obligations involving cybersecurity, including, among other things, the effect of the costs of cybersecurity incidents on a company's financial condition, the description of the company's business, disclosure of material pending legal proceedings, and discussion of the effectiveness of disclosure controls and procedures.

The explosive growth of e-commerce over the past several years has been accompanied by growth in the incidence of credit card and other payment card purchases. Increased use of payment cards has increased the risk of fraud. A consortium of payment card companies has developed the Payment Card Industry (PCI) Data Security Standards, which apply to companies that process, store, or transmit credit card or other payment card information. Although the PCI Data Security Standards are not legislated laws or governmental regulations, they do bind companies pursuant to contractual agreements such as merchant agreements. Accordingly, a failure to comply with these requirements could expose a company to significant financial liability and operational disruption.

Given the gravity of the issues at stake, new media companies must seek to minimize the risk of suffering a security breach, or being targeted for investigation by a regulator or pursuant to a private claim. Even a relatively "less serious" breach in data security could attract widespread public attention and years of expensive, and possibly debilitating, litigation. Damages and reported settlements arising from data security breaches involving seemingly innocuous data, such as only email addresses, have frequently cost affected companies tens of millions of dollars, as well as significant reputational harm.[13] Such settlements for recent incidents involving limited contact information, without traditionally sensitive data like financial or health information, drives home the point: even if you do not handle consumer financial information or social security numbers, you can still suffer significant exposure from losing a large volume of consumer contact information.

Even a relatively "less serious" breach in data security could attract widespread public attention and years of expensive, and possibly debilitating, litigation.

---

11 See, e.g., *In the Matter of BJ's Wholesale Club, Inc.,* FTC No. 042 3160 (June 16, 2005).

12 SEC, Div. Corp. Fin., Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011).

13 See *In re TD Ameritrade Accountholder Litigation*, No. C 07-2852, 2011 BL 234454 (N.D. Cal. Sept. 13, 2011) for an account of an email address security breach at TD Ameritrade, resulting in a settlement for up to $6.5 million. Similarly, a security breach of email databases at Epsilon in 2011 highlighted concerns about outsourcing email marketing to third-parties. Epsilon maintained email address databases for many well-known institutions, who suffered adverse consequences as a result of Epsilon's failure to ensure security of consumer data.

V. Online Agreements and Terms of Use

A. Enforceable Agreements and Terms of Use

Another important legal issue that every new media company faces is ensuring that its terms of use are enforceable. A variety of factors require consideration when evaluating the enforceability of online agreements, including proof of executing an electronic document and authentication of the terms of use and related materials.

New media companies must carefully design the protocol for disclosing and requiring consumer assent to terms of use for their online products or services, in addition to formulating the appropriate provisions of those terms.

Most commonly, new media companies contract with online users via standard form agreements, such as the so-called clickwrap and webwrap agreements. Clickwrap agreements present a user with a message requiring the user to assent with a "click" to the terms of use, while a webwrap agreement involves posting a passive notice on a website, often in the footer, that any user of that website is subject to its terms of use. Such standard form agreements are usually enforceable, provided that the agreement meets certain requirements, such as clarity of terms and adequacy of notice. In contrast, the terms of a clickwrap agreement may not be enforceable if the agreement is not immediately available and presented in such a way that the average consumer would recognize that the agreement exists and understand how to obtain a copy of the agreement.[14] The same issues apply to mobile apps, as well. Ultimately, the firm can protect its value by prescribing enforceable terms of use.

---

[14] *Harris v. Comscore, Inc.,* 2011 U.S. Dist. LEXIS 115988 (N.D. Ill. Oct. 7, 2011).

B. Developer Agreements for Mobile Applications

Development and distribution of mobile apps raise unique issues and require agreement among multiple parties, including the developer, publisher, and app store owner. App stores, which are often operated by mobile platform providers, are the primary conduit for distributing or commercializing a mobile app to consumers. Companies must agree to and comply with developer agreements before submitting their apps for distribution in app stores. Although there is some variation among app store operators, developer agreements are typically standard form contracts that are not open to negotiation. The process of executing developer agreements is usually quick and easy — it may simply involving clicking "Agree" via a clickwrap agreement. The implications of the agreements, however, are far-reaching and complex. Developer agreements often incorporate additional agreements, such as third-party licenses or agreements with the owner of related technology. Thus, despite the ease of entering into the agreement, a mobile app developer must fully understand the terms of the agreement. Failure to comply with developer agreements could result in a costly rejection of the app by the app store operator or a significant increase in development costs, which may ultimately affect the value and profitability of a company.

VI. Conclusion

The quick pace of change and innovation in new media and social media makes investing in the industry equal parts captivating and challenging. Investors should take a holistic approach to their evaluation of potential investments in this industry, paying close attention to business, financial, economic, market, and legal strengths and risks of potential investment opportunities. Accordingly, in addition to procuring sound business and technical advice, investors should also obtain sound legal advice and conduct appropriate legal due diligence of a company before committing to make an investment.

About the Authors

Kristen J. Mathews *is head of the Privacy & Data Security Group and a member of the Technology, Media & Communications Group at Proskauer. Kristen focuses her practice on technology, e-commerce and media-related transactions and advice, with concentrations in the areas of data privacy, data security, direct marketing and online advertising. She regularly advises clients on a wide range of matters, including privacy and data security compliance, customer authentication, responding to data security breach incidents, preparing privacy and data security policies, data profiling, behavioral marketing, open source software issues, financial privacy, children's privacy, international privacy, health care privacy, identity theft prevention, geolocational privacy, mobile marketing, social networking, payment card data security and telematics. She is the editor of the leading treatise in her area "Proskauer on Privacy," published by the Practicing Law Institute, the editor of Proskauer's Privacy Law Blog at www.proskaueronprivacy.com, the editor and author of Proskauer's "A Moment of Privacy" e-newsletter and the chair of Proskauer's annual "Proskauer on Privacy" conference.*

Paresh Trivedi *is a transactional lawyer at Proskauer with more than ten years of experience representing clients in technology, media, communications, cable programming, digital advertising and content distribution transactions and counseling clients on related legal compliance issues. Paresh works in a variety of industries including communications, Internet/e-Commerce, entertainment, television, sports, banking and financial services, publishing, oil and gas, manufacturing, retail, professional services and advertising. He practices in Proskauer's Corporate Department and its Privacy & Data Security, Technology, Media & Communications and Sports Law Groups.*

The authors would like to thank Laura Goldsmith, a summer associate in Proskauer's New York office, for her valuable contributions to this article.


Building a better
working world


NATIONAL
VENTURE CAPITAL
ASSOCIATION
Funding innovation. Empowering entrepreneurs.