INSIDE THE MINDS

Recent Trends in Privacy and Data Security

Leading Lawyers on Analyzing Information Storage Regulations and Developing Effective Data Protection Policies

ASPATORE

For customer service inquiries, please e-mail West.customer.service@thomson.com.

If you are interested in purchasing the book this chapter was originally included in, please visit www.west.thomson.com.

Data Optimization Trends

Kenneth R. Florin

Partner and Co-Chair, Advanced Media and Technology;

Chair, Digital Media

Loeb & Loeb LLP

ASPATORE

Introduction

Many of today's most compelling consumer initiatives involve technology and data. Advertisers can deliver an offer to a consumer's mobile device the moment he or she enters a store. Advertisers use social media platforms to promote a product or to host a contest inviting consumers to submit comments, videos, and photos highlighting their use of a product. Companies around the world deliver ads online and to mobile devices that correlate to a consumer's interests and demographic data. And companies are streamlining the mobile purchasing experience by providing mobile payment systems that can be completed by tapping a mobile device against a merchant's payment reader.

These examples, and many others, depend on technology and data optimization. Data optimization in the advertising and marketing context encompasses the collection and analysis of data from a wide variety of sources that can be used to better understand existing customers, reach potential customers, deliver offers targeted to a consumer's particular interests and location, evaluate products and services, and analyze the effectiveness of advertising campaigns and marketing channels.

The amount of data and the sources of such data have increased exponentially in the last few years, due largely to the Internet and mobile technology. Meanwhile, the laws that govern such data collection and use tend to lag behind technological developments. This means advertisers and marketers are faced with new opportunities in a rapidly changing and somewhat unsettled legal landscape. Companies that want to engage in data optimization may need to begin by determining their comfort level with new technologies when the legal boundaries are not always clear. Some companies will charge ahead, striving to be the first to use a new technology or platform to reach consumers, while others may adopt a wait-and-see approach.

There are several trends in the area of data optimization. First, due in part to the challenges Congress faces in responding quickly to new technology, the states are increasingly leading enforcement and regulatory efforts. Second, self-regulatory programs continue to evolve both for online data

collection and data collection from mobile apps and mobile devices. Third, there is likely to be new federal privacy legislation, although it will most likely be limited to sensitive data, including data from children, and existing federal laws will likely be updated to reflect new technologies.

Technology and data optimization offer opportunities—and challenges—for businesses in the United States. This chapter is designed to give an overview of some of the key legal issues raised by our increasing use of consumer data and current trends in this area. It will highlight some of the existing laws and guidelines that govern these practices and provide examples of legislation that may be enacted in the future. Due to the speed with which new technologies and platforms are adopted, as well as the introduction of new laws and case law, this chapter can only provide a snapshot of these topics as they appear today.

State Enforcement and Legislative Activity

The US Congress is a deliberative body, which means it can take years for Congress to enact legislation that regulates new practices. States are more nimble, which is one reason we are seeing state regulation and enforcement actions relating to data optimization practices.

California has been very active in this area. California was the first state to enact a law requiring commercial websites to provide a privacy policy that described the site's data collection practices.[1] In the last two years, California's attorney general established a Privacy Task Force, entered into a Joint Statement of Principles[2] with the major mobile app marketplaces setting forth privacy protections, issued a set of mobile privacy guidelines[3],

[1] California Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575-22579 (2003).
[2] California Office of the Attorney General, *Joint Statement of Principles* (Feb. 22, 2012), http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf. Entered into between the California Attorney General and the companies whose platforms comprise the majority of the mobile app market (Amazon, Apple, Facebook, Google, Hewlett-Packard, Microsoft, and Research In Motion), the Principles require mobile apps to disclose their data collection practices, and require mobile app marketplaces to provide a link or other access mechanism to an app's privacy policy and a mechanism for consumers to report non-compliance.
[3] ATTORNEY GENERAL'S PRIVACY ENFORCEMENT AND PROTECTION UNIT, CALIFORNIA DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (Jan. 2013), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

and announced the state's first enforcement action alleging a mobile app violated the state's Online Privacy Protection Act by neglecting to provide a privacy policy.

The mobile privacy guidelines, titled *Privacy on the Go: Recommendations for the Mobile Ecosystem*, were issued in January 2013.[4] Most of the recommendations are directed to mobile app developers, but there are also recommendations for others in the industry, including hardware manufacturers, operating system developers, mobile telecommunications carriers, and advertising networks. A recurring theme in the recommendations is to "minimize surprises to users from unexpected privacy practices." Recommendations include: (1) mobile apps should avoid collecting personally identifiable data from users that are not needed for an app's basic functionality, and (2) app developers should supplement a general privacy policy "with enhanced measures to alert users and give them control over data practices that are not related to an app's basic functionality or that involve sensitive information." Such enhanced notice and control might be provided through special notices that are delivered in context and "just in time." For example, operating systems that use location data can deliver a notice just before collecting the data and give users an opportunity to allow or prevent the practice. The report also provides a checklist for building privacy into app development.

A few weeks after the mobile privacy guidelines were issued, California Assembly Bill 257 was introduced.[5] The bill, if enacted, would codify many of the best practices proposed by the California attorney general's report on mobile privacy, such as requiring mobile apps to have a privacy policy; allowing consumers to access their own personally identifiable information (PII) that the app collects and retains; provide a supplemental privacy policy with enhanced measures if an app collects PII that is not essential to the app's basic function; providing a special notice if the app accesses text messages, call logs, the camera, dialer or microphone, or collects location, financial, or medical information or passwords. The bill also would require advertising networks that deliver ads through a mobile application to obtain prior express consent before displaying an ad and before accessing PII; use application-specific or temporary device identifiers rather than unchangeable device-

[4] *Id.*
[5] A.B. 257, 2013 Leg., Reg. Session (Cal. 2013).

specific identifiers; and transmit user data securely, using encryption for permanent unique device identifiers and personal information.
Another bill was introduced (Assembly Bill 242)[6] that would amend California's Online Privacy Protection Act by requiring that privacy policies be no more than one hundred words long, be written in clear and concise language that an eighth grader could read, and indicate whether PII may be sold or shared with others, and how and with whom the information may be shared.

In 2012, California enacted a law prohibiting employers in California from asking or requiring employees or job applicants to provide their log-in credentials for social media sites such as Facebook, Tumblr and Twitter. California's Social Media Privacy Act,[7] one of the most comprehensive social media privacy laws in the nation, went into effect on January 1, 2013, and adds provisions to California's existing Labor Code that prohibit all employers—both private and public—from demanding usernames or passwords for the purpose of accessing personal social media accounts or from requiring an employee or applicant to access personal social media in the presence of the employer or to divulge any personal social media. Under the new law, employers may not discipline, discharge, threaten those actions, or otherwise retaliate against an existing or prospective employee for failing to comply with a demand that violates the law. The law does not prohibit employers from demanding credentials to access an employer-provided piece of equipment, however.

States have also been very active in enacting data security and security breach notification laws. Massachusetts was one of the first states to enact a strict data security law[8] which requires, among other things, companies that own, license, store or maintain personal information about a Massachusetts resident to: (1) develop, implement and maintain a comprehensive, written information security program; (2) implement physical, administrative and extensive technical security controls, including the use of encryption; and (3) verify that any third-party service providers that have access to personal information can protect such information. Security laws like this require companies to revisit contracts with vendors that have access to data, train employees in data security

[6] A.B. 242, 2013 Leg., Reg. Session (Cal. 2013).
[7] CAL. LAB. CODE § 980 (2012).
[8] Standards for the Protection of Personal Information from Residents of the Commonwealth, 201 MASS. CODE REGS. § 17.00 (2009).

procedures, and examine how they collect, use, share and store data across a growing number of platforms and delivery systems.
It is important to keep in mind that the Federal Trade Commission (FTC) has also been active in utilizing Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce[9], to protect consumers' data. The FTC has brought over one hundred enforcement actions[10] under Section 5 against companies that failed to comply with their own privacy policy, changed their privacy policy without offering consumers a chance to opt-out of the new changes, failed to adequately safeguard data, failed to adequately disclose what data is collected and for what purpose, and failed to honor opt-out promises.

In February 2013, the FTC announced a settlement with the developer of a social networking website and mobile app called Path. The FTC alleged that Path improperly collected personal information from users' mobile address books without their knowledge or consent. Specifically, the FTC charged that the user interface in Path's iOS app was misleading and provided consumers no meaningful choice regarding the collection of their personal information. The Path app offered an "Add Friends" feature to help users add new connections to their networks. The feature provided users with three options: "Find friends from your contacts;" "Find friends from Facebook;" or "Invite friends to join Path by e-mail or SMS." According to the FTC, Path automatically collected and stored personal information from the user's mobile device address book even if the user had not selected the "Find friends from your contacts" option. For each contact in the user's mobile device address book, Path automatically collected and stored any available first and last names, addresses, phone numbers, e-mail addresses, Facebook and Twitter usernames, and dates of birth. The FTC also charged that Path, which collects birth date information during user registration, violated the Children's Online Privacy Protection Act (COPPA) Rule[11] by collecting personal information from approximately 3,000 children under the age of thirteen without first getting parents' consent.

[9] 15 U.S.C. § 45(a) (2012).
[10] *Legal Resources,* FTC BUREAU OF CONSUMER PROTECTION BUSINESS CENTER, http://business.ftc.gov/legal-resources/29/35 (visited Feb. 27, 2013).
[11] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06, 16 C.F.R. pt. 312.

The FTC also enforces the Safeguards Rule,[12] which establishes standards intended to ensure the security and confidentiality of financial customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information. The Rule requires, among other things, companies to develop a written information security plan that describes their program to protect customer information and to assess and address the risks to customer information in all areas of their operation, including employee management and training; information systems; and detecting and managing system failures.

Self-Regulation Evolves

In the last three years, there has been significant growth in the self-regulation of data optimization practices. The Digital Advertising Alliance,[13] comprised of advertising trade groups and individual advertisers, has developed several self-regulatory guidelines and many in the advertising industry are participating in these programs. The DAA's self-regulatory principles for online behavioral advertising require: (1) notice to consumers when behavioral information is collected or used; (2) opt-out for the collection and use of data for online behavioral advertising purposes by third-party ad serving networks and websites where the data is collected, except opt-in for the collection and use of sensitive data (i.e., data from children under thirteen and financial and medical data) and for data collected by service providers; (3) opt-out mechanism should last for a minimum of five years; and (4) all entities should obtain consent before applying any material change to their online behavioral advertising data collection and use policies prior to such change.[14]

The Council of Better Business Bureaus (CBBB) and the Direct Marketing Association (DMA) monitor compliance. In 2012, the CBBB's Accountability Program announced compliance decisions involving Kia

[12] Standards for Safeguarding Customer Information;16 C.F.R. pt. 314.

[13] Digital Advertising Alliance is comprised of the American Advertising Federation (AAF), Association of National Advertisers (ANA), American Association of Advertising Agencies (AAAA) and hundreds of individual advertisers.

[14] *About the Self-Regulatory Principles for Online Behavioral Advertising*, THE SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, http://www.aboutads.info/obaprinciples.

Motors, its media agency (Initiative), and two advertising networks that served Kia ads (Specific Media and Rocket Fuel). The Accountability Program determined that certain Kia ads were served without the required notice and choice mechanism. The CBBB announced more than a dozen compliance actions in 2011 and early 2012: some advertisers failed to honor opt-out requests for the industry minimum of five years, others failed to have working opt-out links, and one company did not clearly explain that its device identification technology gave it the capability to collect and use data for OBA across multiple devices in a household, and it did not tell consumers what further steps they would have to take to opt out for all other devices they use.

Another area with growing self-regulation is mobile privacy and security. The DAA is working on a new set of self-regulatory guidelines for mobile apps. The Mobile Marketing Association issued mobile app privacy guidelines in 2010 and the FTC released three sets of guidelines for mobile app developers in 2012.

The FTC's *Mobile Privacy Disclosures: Building Trust Through Transparency*[15] includes recommendations for best practices for key players in the mobile "ecosystem": mobile platforms, app developers, advertising networks, and other third parties such as analytics companies that collect and use data from mobile apps. The recommendations are intended to address the challenges of providing effective, accessible, and timely privacy disclosures on mobile devices, given the limitations of mobile technology, including the small screen on most devices and the limited attention span of users.

In *Marketing Your Mobile App: Get It Right from the Start*,[16] the FTC provides guidance to help mobile app developers comply with truth-in-advertising standards and basic privacy principles when marketing new mobile apps. The guidance is intended for all mobile app developers—large companies as well as tiny start-ups and individuals. Stating that there is no one-size-

[15] FEDERAL TRADE COMMISSION, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), *available at* http://www.loeb.com/files/Uploads/mobileprivacyreport.pdf.

[16] *Marketing Your Mobile App: Get It Right From the Start*, FTC BUREAU OF CONSUMER PROTECTION BUSINESS CENTER, http://business.ftc.gov/documents/bus81-marketing-your-mobile-app.

fits-all approach and that every app is different, the Commission provided some general guidelines that all app developers should consider such as tell the truth about what your app can do, disclose key information clearly and conspicuously, build privacy considerations in from the start, offer choices that are easy to find and easy to use, honor your privacy promises, protect kids' privacy, and keep user data secure.

The FTC's *Mobile App Developers: Start with Security*[17] suggests mobile app developers protect data by making someone responsible for security, take stock of the data collected and retained, and use transit encryption for usernames, passwords, and other important data.

The National Telecommunications and Information Administration has been convening multi-stakeholder meetings to develop a mobile app transparency Code of Conduct. This initiative was established by the Obama administration's Consumer Privacy Bill of Rights, released in February 2012.[18] A discussion draft of the Code of Conduct[19] calls for mobile app developers to provide standardized, short form notices that detail the app's data collection and data sharing practices.

While many business interests in the United States prefer self-regulation to new laws, the growing number of guidelines and self-regulatory programs highlights the need for careful planning. A company should determine whether it is subject to a certain group's guidelines and it may need to implement new technology and procedures to comply with a self-regulatory program. And if a company chooses to use a self-regulatory icon to indicate its adherence to certain guidelines, it should make sure its data practices are actually aligning with the self-regulatory program's guidelines.

---

[17] *Mobile App Developers: Start with Security,* FTC BUREAU OF CONSUMER PROTECTION BUSINESS CENTER, http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

[18] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[19] NTIA Multistakeholder Process: Mobile App Transparency, National Telecommunications & Information Administration (Feb. 21, 2013), http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

Enacting and Updating Federal Privacy Laws

Dozens of laws already exist that regulate data collection, use, sharing, and security at the federal and state level, but many of these were enacted before today's most popular technologies were adopted. In addition to drafting new laws, rules and regulations, legislators and regulators are working to update some existing privacy laws to encompass new technologies and practices. The FTC just completed a three-year project to update the Children's Online Privacy Protection Act (COPPA)[20], which applies to the online collection of personal information from children under thirteen and requires, among other things, that web site operators obtain parental consent before collecting such information. Specifically, the FTC was concerned that COPPA did not keep pace with how children are using technology and how companies are using technology to collect information from children.

In December 2012, the FTC announced the final version of its changes to its COPPA Rule. These changes are likely to have a significant impact on a wide variety of companies. For example, the definition of "personal information," was expanded to include geolocation information, photographs, videos and audio files that contain a child's image or voice, screen or user names in cases in which these identifiers function as online contact information (defined as an e-mail or other identifier that permits direct online contact with a user), and "persistent identifiers" (a user number held in a cookie, an Internet protocol (IP) address, a processor or device serial number, or unique device identifier), that can be used to identify users over time and across different websites or online services. Also, the definition of "website or online service directed to children" was revised to extend the parental notice and consent requirements to those third parties, such as providers of plug-ins and ad networks, that collect personal information when those third parties have

[20] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06 (1998) and the FTC's COPPA Rule (16 C.F.R. pt. 312) require operators of commercial websites and online services directed to or knowingly collecting personal information from children under 13 to: (1) notify parents of their information practices; (2) obtain verifiable parental consent before collecting a child's personal information; (3) give parents a choice as to whether their child's information will be disclosed to third parties; (4) provide parents access to their child's information; (5) let parents prevent further use of collected information; (6) not require a child to provide more information than is reasonably necessary to participate in an activity; and (7) maintain the confidentiality, security, and integrity of the information.

actual knowledge that they are collecting personal information through a child-directed website or online service.

Several federal bills have been introduced that would regulate mobile privacy. Rep. Ed Markey (D-Mass.) introduced the Mobile Device Privacy Act (H.R. 6377)[21] which would require disclosure of the use of monitoring software on mobile devices; consent to the collection of information, including a user's location, that is collected using monitoring software; and information security policies and procedures to safeguard collected data.

The bill authorizes the FTC to promulgate regulations that would require certain entities to make clear disclosures about the use of monitoring software with the capacity to monitor the use of a mobile device or the location of the user and to transmit the information to another device or system. The disclosure requirements would apply to sellers of mobile devices that have monitoring software installed on the device, certain providers of commercial mobile or data services, manufacturers of mobile devices or mobile operating systems that install monitoring software on a device after it is sold to a consumer, and operators of websites where consumers can download monitoring software for mobile devices. These entities would be required to make the following disclosures:

1. The fact that monitoring software is installed on the mobile device, or the fact that the software the consumer is downloading is monitoring software;
2. The types of information the monitoring software is capable of collecting and transmitting;
3. The identity of any person who receives such information;
4. How such information will be used; and
5. Procedures for consumers who have consented to such collection and transmission to opt out of future collection and transmission.

If the bill were enacted, those subject to the disclosure requirements would be required to obtain the express consent of consumers prior to any data collection by monitoring software and to provide consumers who have consented to the collection and transmission an opportunity to opt out of

[21] H.R. 6377, 112th Cong. (2012).

future collection and transmission. The law would also authorize the FTC to require anyone who directly or indirectly receives information transmitted from monitoring software that is subject to the disclosures to establish and implement policies and procedures for safeguarding that information. The Mobile Device Privacy Act would be enforced by the FTC, FCC, and state attorneys general. The bill also permits a private right of action whereby consumers could be compensated up to $3,000 per violation if those violations are deemed willful or knowing.

Helping Clients Navigate Data Privacy Rules and Regulations

To help clients navigate existing data privacy rules and regulations, it is important to conduct regular data audits. These audits examine how information has been or will be obtained, how it flows, and how it will be utilized. Understanding these issues is important to safely conduct data optimization. But it can also be helpful in M&A and other transactions involving companies that are valued significantly based on their data. Companies, and investors in such companies, might not understand the opportunities and hurdles that may exist now or in the foreseeable future related to data that is key to valuing investments. And data audits can be critical in developing this information. Companies and investors need to understand what data the target company owns or has access to; how it was obtained and from whom; and how that data will be used going forward.

A data privacy/protection compliance strategy will vary greatly, depending upon the client's industry and size of the company. For example, to the extent that the client's industry processes sensitive information—i.e., health-related or financial data—counsel needs to be even more rigorous in assessing what restrictions there are on sensitive data. Also, to the extent that a company is international rather than domestic, counsel needs to consider the laws and regulations in multiple jurisdictions. When clients are engaging in international platforms, counsel should have professionals on their team who are competent in terms of assessing the international regulatory environment, and that might mean understanding more than the letter of the law. Rather, counsel needs to know how the law is complied with by companies that are actually operating in a certain country.

Conclusion

Technology creates opportunities—and challenges. Technology has allowed companies to reach consumers in new ways, and to make that a two-way conversation. Advertisers now have the ability to deliver ads and offers to consumers they know are interested in their products, and to measure how effective their advertising and marketing campaigns are on a granular level. At the same time, the amount and type of data that is used in new forms of advertising are a concern of regulators and legislators. The challenge for companies and their lawyers is understanding the many sources of privacy and security regulation (state, federal, and local laws; self-regulatory guidelines; industry best practices; platform and carrier policies; international laws; and a company's own privacy policy), and knowing how new products and services deploy emerging technologies to collect, share, and use data.

Key Takeaways

- Data optimization is a rapidly evolving area of the law. Lawyers practicing in this area need to stay up-to-date on all developments relating to privacy including new laws, guidelines, case law, class action complaints, and state, federal, and self-regulatory enforcement actions, in all the jurisdictions where a client is conducting business.
- Keep in mind that privacy and data security laws vary greatly in other countries with respect to the level of transparency, the nature of consent or choice, and the penalties for failure to comply with the law. Clients who transfer data electronically on an international basis need to consider where the information is coming from; where it is going to; where the servers are located; what is the purpose behind the use of the information; who is providing the information; what is the nature of the information being provided; and whether certain privacy laws, privacy policies, or other statements restrict or in any way define how that information can be collected and used.
- Keep in mind that many clients who are involved in M&A activity want to invest in companies that have valuable data, but they may not have a real understanding of how that data was obtained, how it can be used, how it was used in the past, and

how it may be used in the future.

- Regularly review and update all of a client's existing compliance programs. Develop a strategy that takes into account existing and likely to be adopted laws or regulations; and make sure that the client is aware of any material changes that are taking place in jurisdictions that matter to them.

Related Resources

Online Behavioral Advertising

- Digital Advertising Alliance (DAA) *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), http://www.aboutads.info/obaprinciples
- DAA *Self-Regulatory Principles for Multi-Site Data* (November 2011), http://www.aboutads.info/msdprinciples
- Council of Better Business Bureaus Online Interest-Based Advertising Accountability Program, http://www.bbb.org/us/interest-based-advertising
- Interactive Advertising Bureau (IAB) *Privacy Principles* (February 2008), http://www.iab.net/guidelines/508676/1464
- Direct Marketing Association (DMA) *Guidelines for Ethical Business Practices* (May 2011), http://www.dmaresponsibility.org/guidelines/

Mobile Privacy

- FTC *Marketing Your Mobile App: Getting It Right from the Start* (September 2012), http://business.ftc.gov/documents/bus81-marketing-your-mobile-app
- FTC *Mobile Privacy Disclosures: Building Trust Through Transparency* (February 2013), http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf
- FTC *Mobile App Developers: Start with Security* (February 2013), http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security

- Wireless Association (aka CTIA) *Best Practices and Guidelines for Location Based Services* (March 2010), http://www.ctia.org/business_resources/wic/index.cfm/AID/11300
- Mobile Marketing Association (MMA) *Code of Conduct for Mobile Marketing* (July 2008), http://www.mmaglobal.com/bestpractice
- MMA *Mobile Application Privacy Policy Framework* (December 2011), http://www.mmaglobal.com/node/18771?filename=MMA_Mobile_Application_Privacy_Policy_15Dec2011PC_Update_FINAL.pdf
- National Telecommunications and Information Administration Mobile Application Transparency Code of Conduct (draft), http://www.ntia.doc.gov/other-publication/2013/privacy-multi stakeholder-process-mobile-application-transparency

Children's Online Privacy Protection Act (COPPA)

- Federal Trade Commission (FTC) Revised COPPA Rule (December 2012), http://www.ecfr.gov/cgi-bin/text-idx?SID=792816084b3962da246cd840923ba361&node=20130117y1.14

California

- California Office of Privacy Protection (provides a comprehensive list of all California and some federal privacy laws) http://www.privacy.ca.gov/
- California Online Privacy Protection Act (2003), http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579
- California Attorney General Joint Statement of Principles for Mobile App Markets, http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf
- California Attorney General *Privacy on the Go: Recommendations for the Mobile Ecosystem* (January 2013), http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf?

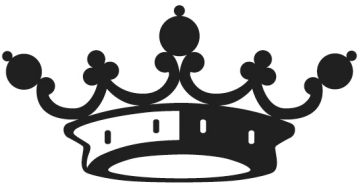
Kenneth R. Florin is a partner at Loeb & Loeb LLP, co-chair of Advanced Media and Technology, and chair of Digital Media. Kenneth is one of the industry's leading experts on matters involving the convergence of advertising, technology, emerging media, and privacy. In addition to a rich background in traditional marketing and communications, he has been a pioneer in counseling clients on the use of new technologies, digital media, international promotions, and emerging content distribution models that companies are increasingly using to extend their global reach.

Mr. Florin represents Fortune 500 companies, media companies, advertising and promotions agencies, social media platforms, sports leagues and teams, and new media and interactive ventures, advising them on the development of their advertising and promotion strategies, online communities, wireless and social media initiatives, and technology-related products and services. He negotiates deals ranging from traditional agency-client, co-promotion, tie-in, and employment and sponsorship agreements to licensing deals for the digital distribution of content, Internet and e-commerce development agreements, and multi-platform branded entertainment agreements. Mr. Florin reviews concepts, layouts, and copy for all forms of advertising and promotion initiatives, including sweepstakes and contests, wireless and interactive promotional campaigns, cause-related marketing programs, and auctions. He has extensive experience in the area of international promotions. In addition, Mr. Florin assists his clients in the development of their data collection and privacy policies, targeted advertising matters, in the handling of regulatory and consumer inquiries and complaints, and with trademark and copyright issues.

ASPATORE

Aspatore Books, a Thomson Reuters business, exclusively publishes C-Level executives and partners from the world's most respected companies and law firms. Each publication provides professionals of all levels with proven business and legal intelligence from industry insiders—direct and unfiltered insight from those who know it best. Aspatore Books is committed to publishing an innovative line of business and legal titles that lay forth principles and offer insights that can have a direct financial impact on the reader's business objectives.

Each chapter in the *Inside the Minds* series offers thought leadership and expert analysis on an industry, profession, or topic, providing a future-oriented perspective and proven strategies for success. Each author has been selected based on their experience and C-Level standing within the business and legal communities. *Inside the Minds* was conceived to give a first-hand look into the leading minds of top business executives and lawyers worldwide, presenting an unprecedented collection of views on various industries and professions.



ASPATORE