

Key Privacy, Security and Information Management Issues in a Digital World Economy

Douglas S. Pulitzer
dpulitzer@ingramllp.com

Web 2.0, mobile applications and cloud based services have revolutionized how companies communicate and interact with customers, current and prospective, and how businesses process, transmit, secure and store information. However, the experiences of Google, Facebook, Amazon and other digital giants also demonstrate the pitfalls for business in a digital world economy.

Here are suggestions on how to address fundamental requirements necessary to achieve the best privacy, security and information management practices in a digital world economy:

1. **Privacy by Design.** Companies must incorporate meaningful privacy protections into their daily information practices, throughout the life cycles of their products and services. These include, but are not limited to, making certain that data is adequately secured, setting reasonable collection limits, obtaining affirmative consents, having sound retention, use and sharing practices, and implementing procedures to insure data availability, accuracy and notification.

Suggestion: Designate specific personnel who: (i) oversee privacy issues from the earliest stages of research and development, (ii) are responsible for training employees on privacy, and (iii) promote and enforce accountability for privacy policies throughout the company. Assess the privacy impact of practices, products, and services to evaluate risks and ensure that the company follows appropriate procedures to mitigate those risks.

2. **Know Your Company's Partners, Affiliates and Vendors.** Your company's information sharing and processing requirements can involve a complex network of parties associated through various types of legal relationships, including: hosting, transaction, cloud and communications providers; corporate affiliates; marketing partners; retailers; wholesalers; and advertisers. In addition to standard contract issues such as warranties, deliverables, indemnification and liability, it is important to fully understand how your company's and customers' proprietary and personal information is being used by such third parties and the risks and exposures placed upon your company from such usage.

Suggestion: Make sure that your company's information use, storage, sharing, transmission and securitization (encryption) policies and requirements are being followed. It is important to clearly specify: (i) where your company's information may reside or be transmitted, (ii) who may access and use your company's information during and after the agreement, and (iii) who is responsible for data security breaches and for compliance with applicable security notification breach laws.

3. **Cloud-Based Services.** Cloud computing can provide a scalable on-demand combination of hardware, software and services. However, in taking advantage of the efficiency and cost savings offered by cloud computing, your company's mission-critical IT-enabled services must still be configured to provide adequate failover capabilities, and service levels that will support the operational and risk exposure imperatives of your company's information technology and use requirements.

Suggestion: When utilizing cloud solutions, companies should configure their cloud services in a way that eliminates single points of failure and demand operationally meaningful service level commitments. These service level commitments should include, at a minimum, (i) clearly defined service availability, integrity and security standards, (ii) commitments to respond to, resolve and report any service problems in a timely manner (including applicable regulatory requirements, such as reporting any computerized data

breaches under federal and/or state law), and (iii) service credits and other remedies if the provider fails to meet these service levels. In the event your company cannot obtain adequate contract terms, it may be worthwhile to consider purchasing a comprehensive cyber insurance policy. Such a policy should cover the computer networks directly under the control of the company and those computer networks operated by the cloud provider for or on behalf of the company. Appropriate cyber insurance coverage should provide a fallback risk transfer and relieve the company of retaining undesirable risk.

- 4. Mobile Application Privacy Requirements.** When customers install a mobile application with your company's name and logo, they expect your company to adequately safeguard the personal and sensitive information they keep on their phones. Breaching that trust may harm a company's reputation, in addition to giving rise to legal repercussions.

Suggestion: It is important that users of your company's mobile application(s) are aware of, and explicitly accept during installation, how the application uses their personal and sensitive information. In addition, if you hire a third party to develop your company's branded mobile application, ensure that the developer agreement states your company's information use and securitization (encryption) requirements and adequately protects your company from any developer's failure to comply with these requirements. The Mobile Marketing Association's recent *Final Privacy Policy Guidelines for Mobile Apps* ("**Guidelines**") provides a general starting point for application developers when drafting their application privacy policies. The Guidelines include model language regarding the application's and developer's privacy practices, as to: (a) what information is collected, and how it's used; (b) whether the app collects location-based information; (c) whether third parties have access to any information; (d) whether consumers can opt-out of information collection or sharing; (e) how long information is retained; (f) whether the app is directed to children under 13; and (g) how information is safeguarded. However, your company and its developers mustn't simply rely on the Guidelines language; they must still draft a privacy policy to address the company's unique, application-specific privacy practices and display it in prominent fashion and in easy to understand language before the app is downloaded. Inaccurate or deceptive privacy policies are subject to actions by the Federal Trade Commission, state Attorneys General and other regulators. See point 5.

- 5. Up-to-Date and Compliant Privacy Policies.** Public facing privacy policies can quickly become obsolete as your company adds new online offerings or tracking technologies, or changes the way it handles personal and sensitive information in response to new opportunities. An outdated policy poses legal risks, as falling short of its promises could be an "unfair or deceptive trade practice." Both the Federal Trade Commission and state Attorneys General have pursued failures to comply with privacy policies, which are binding public representations about how a company will deal with personal and sensitive information.

Suggestion: Annually conduct a thorough review of how your company collects, uses and shares personal and sensitive information via its website, mobile apps and other online services. Such an annual audit should examine whether your company's published privacy policies reflect actual data usage practices and are reasonably comprehensive, easy to read and easy to access. At a minimum, make certain your company's published privacy policies clearly state what type of information your company collects, who may provide information, how it uses, stores and secures this information and how these benefit the consumer, who it may share this information with, how an individual may access or request changes to such information, the policy's effective date. It is also imperative to provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner than stated when the data was collected.

- 6. Information Security Program (ISP).** An ISP should provide a comprehensive means to ensure compliance with applicable requirements.

Suggestion: An ISP should include, at a minimum, (i) administrative, technical, and physical safeguards to protect the availability, security, confidentiality and integrity of the personal information maintained by the company, including consumer and employee data, at each stage in the information flow, from collection through disposition; (ii) managerial coordination and accountability, including personnel from legal, human resources, information technology, audit and each of the business units involved; (iii) procedures and standards for third parties that access the company's personal information, including due diligence and guidelines relating to specific privacy, confidentiality and information security requirements from such parties; and (iv) a systematic approach to identifying and responding to security incidents involving personal information maintained by the company, including investigation, notification and resolution procedures, and making changes to any existing practices that may have led to the security incident.

- 7. Encrypt:** Sensitive information must be encrypted for storage and transmittal over a secure connection. In addition, the method of clearing, purging or destroying the media used to store sensitive information must prevent the information from being retrieved in a usable, readable or decipherable manner. This is required by several laws and industry body regulations, including the Payment Card Industry Standards (for credit card information), the Massachusetts data security regulations, and the HITECH Act (for electronic protected health information).

Suggestion: Ensure that your company adopts encryption and transmission policies that comply with encryption standards such as: (i) for data at rest, National Institute of Standards and Technology (NIST) Special Publication 800-111; and (ii) for data in transit, Federal Information Processing Standard 140-2. The method of clearing, purging or destroying the media used to store sensitive information should also comply with standards such as NIST Special Publication 800-88.

To discuss best privacy, security and information management practices, please contact Douglas Pulitzer whose practice specializes in privacy, security, information management, outsourcing, technology and ecommerce.

Douglas Pulitzer became counsel to the firm in 2010. Douglas has practiced law for over 20 years and has expertise concentrated in technology, ecommerce, mcommerce, social media, privacy, information management and intellectual property law (collectively, "Expertise"). He represents a broad range of clients, from start-up entrepreneurs to multinational corporations.

He has enjoyed a wide variety of legal experiences over his career that have provided him with a unique perspective and legal skill set, including work at a large Wall Street law firm, in-house experience at both a Global financial services firm and a revolutionary beverage company, and the entrepreneurial endeavor of running his own law firm.

Douglas has extensive experience in structuring, drafting and negotiating a wide range of transactions in matters related to his areas of Expertise which include: advising companies on issues of moving to a Web 2.0-based environment and implementing an ecommerce and mcommerce infrastructure, social media issues, privacy and data security

assessments, compliance and policies, including cross-border data transfers and the strategic collection and management of personal information assets; creation and structuring of strategic alliances, joint ventures and other partnership arrangements; complex licensing and cross-licensing agreements; design, development and distribution agreements; service level agreements; agreements for technology-related services; data center lease agreements; co-location agreements; procurement (government and commercial for both tangible and intangible items); outsourcing transactions, including help desk, planogram, category management, cloud computing, and software as a service; open source issues, marketing and co-branding agreements; publishing and collaboration agreements; and strategic intellectual property and information asset purchases, sales, use, transfer, management and protection.