White Paper

Protecting Brand Reputation Through Third-Party Assurance of Information System Security and Data Privacy Best Practices

TABLE OF CONTENTS

Purpose 2
Background 2
Engagement 3
Staffing 4
Appendix A 5

iCompli, division of BPA Worldwide
100 Beard Sawmill Road, 6th Floor, Shelton, CT USA I +1.203.447.2800 I www.bpaww.com

PURPOSE

This case study is based on an iCompli engagement which took place over several weeks in mid-2012. Due to the sensitivity of the engagement, the client has requested the company name remain confidential. However, the company is a publicly traded corporation with headquarters in the US and doing business around the world. It is part of the Standard and Poor's 500 Index.

BACKGROUND

iCompli is a division of BPA Worldwide, a not-for-profit audit organization in the Business of Providing Assurance (BPA) since 1931. Its legacy business is setting audience measurement standards for publications and newspapers, online media, and event attendance and then auditing to those standards. BPA Worldwide is the only global, not-for-profit auditor of print, on-line and in-person media. Now in its 81st year, BPA audits more than 2,600 media properties in more than 30 countries around the world with Libya, South Africa, Tanzania and Vietnam as our most recent additions. Full service offices are located in Beijing, Dubai, London, Montreal, Toronto, Shenzhen and headquarters in Shelton, Connecticut (nearby New York City).

The iCompli division provides services that document compliance to defined standards and provides independent, third-party verification of technology or service claims. Customized audit engagements are performed by staff auditors fully certified in specific areas of compliance testing. iCompli verifies adherence to the recommended guidelines of industry bodies and government regulations, as well as self-declared or internal policies and controls.

iCompli engagements are performed in accordance with best practices as defined by GUARDS (Gathering-Usage-Association-Restriction-Demonstration-Strategy), a process developed by noted consultancy Web Analytics Demystified and follows ISO/IEC 27001 protocols. Engagement objectives include:

- Enabling senior leadership, corporate boards, and shareholders to understand where consumer data is being collected;
- Identifying *how* digitally collected consumer data is used for internal marketing or other business pursuits;
- Provides independent third-party assurance that consumer data governance is meeting ethical best practices for digital data privacy.

GUARDS assurance is the first step towards demonstrating the businesses commitment to consumer data privacy. Systems that can be examined for both actively- and passively-collected consumer data include:

- Web Analytics (i.e. Adobe Omniture, Webtrends, Google Analytics)
- Voice of Customer (i.e. ForeSee Results, OpinionLab, iPerceptions)
- Customer Experience Management (i.e. Tealeaf, Clicktale)
- Testing and Targeting (i.e. Adobe Test&Target, Monetate, SiteSpect)
- Audience Panels (i.e. comScore, Quantcast)Personalization (i.e. Adobe 1:1, Baynote, Certona)
- Cloud-based Data Collectors (i.e. Domo, Anametrix)
- Advertising (i.e. Double-Click, Marin Software)
- CRM & Marketing Automation (i.e. Salesforce.com, Eloqua, Marketo)

BACKGROUND *Continued)*

- E-mail Marketing (i.e. Responsys, ExactTarget, Epsilon)
- Social Media Tools & APIs (i.e. Facebook "Like", YouTube)

With mounting concern about consumer data privacy online, iCompli offers a comprehensive internal audit of enterprise systems having digital consumer touch-points.

ENGAGEMENT

The client contracted with iCompli to receive an independent analysis of practices related to data collection, processing and use. The review was performed in accordance with GUARDS consumer digital data privacy best practices and included:

- Identifying Consumer Touch-Points
- Identifying Consumer Data Collectors
- Identifying Consumer Data Collected
- Evaluating Consumer Data Use
- Review of Internal Controls of Data Protection, Privacy, Access Control, Risk Assessment/ Management and Consumer Disclosures

The scope of the engagement did not extend beyond the client to include a review of internal controls of third-party vendors/partners.

In addition, as a global corporation, the client was sensitive to the requirements of the 2011 European Union ePrivacy Directive. In accordance, iCompli was asked to:

1) Review the client's public privacy statement to ensure transparency in the site's use of cookies and passive data collection practices. Further, the privacy statement was to provide details on how to opt out and delete cookies and how to manage "do not track" (DNT) settings in modern browsers.
2) Provide a recommendation to redirect visitors who have DNT checked in their browsers to a special transitional page for an explanation of cookie implementation and to allow an option to allow for cookie placement.
3) Examine the client's current practice to exclude from cookie placement and passive data collection programs any website visitors from countries whose laws require prior consent or obtain consent through an implementation similar to that described in #2 above.

The audit phase of this engagement was a five-step process:

- **Step 1: Identify Consumer Data Touch-Points**
  This initial step included a fact-finding exercise of discovery to identify all consumer touch-points owned, managed, or benefitting the client organization.
- **Step 2: Identify Consumer Data Collectors**
  Step 2 consisted of a complete assessment of the digital data collection technologies used across these touch-points. This process included a combination of automation software tools and human verification, the latter being done both independently (i.e. qualified iCompli personnel resources scanning pages and code) and in combination with the client (i.e. asking directly, "What do you use to collect consumer data?").

ENGAGEMENT *Continued)*

- **Step 3: Identify Specific Consumer Data Collected**
  Step 3 involved a very granular audit of the actual data being collected. This required temporary logins to all of the systems identified in Step 2 to review, evaluate, and document the entire range of data collected via each system. Examination was for specific consumer data typically collected using "custom" variables in the systems in question. The dimensions used to describe this data were as follows:
  - **Gathering**: Extrapolated, Passively Collected, Explicitly Collected
  - **Usage**: Anonymous, Segment Identifiable, Personally Identifiable
  - **Association**: Aggregated, First-Party, Third-Party
- **Step 4: Evaluate Consumer Data Use**
  Based on the results of Step 3, an assessment was created detailing how the data is used within the business. To create this summary, interviews were conducted with client resources who have ownership over or visibility into, the collection systems and data, including business and customer intelligence (BI/CI), CRM, and other data and analytics workers to ensure a complete understanding of the data and its movement across the business is complete.

  A complete list of the privacy, data, and access controls audited during the GUARDS process is included in *Appendix A* of this document.
- **Step 5: Present Results**
  The presentation of GUARDS results included a high-level summary of findings highlighting those issues that needed to be corrected; the output from Steps 1 through 4; and an appendix of all sources used during the audit process. Where possible, the results summary contained screenshots clearly highlighting identified consumer data with notes about the system and any logins/set-up information required so that the client could easily duplicate the views presented.

STAFFING

The engagement was performed by two iCompli staff members. The lead auditor was a director, electronic audit services, with 13 years auditing experience, BA degree and a Certified Information System Auditors (CISA). He was supported by an analyst, electronic audit, with 5 years auditing experience, BA degree in computer science and a CISA. The completed work was reviewed by a senior vice president, audit operations, with 20 years auditing experience and who is a licensed CPA and CISA.

For more information regarding this case study or any iCompli services, contact Chuck Sweeney, Manager, Business Development, iCompli at: +1 (203) 447-2814 or csweeney@bpaww.com

APPENDIX A

The following is an overview of aspects of the client's business that were examined as part of the GUARDS audit. The elements to be examined are customized to meet the client's needs.

PRIVACY AND DATA PROTECTION CONTROLS

- Review privacy policy document/disclosure
  - Confirm consistency of the privacy policy with actual practices
- Overview of data collection/risk exposure
  List all personal information points collected/stored by system
  - Review different levels of sensitivity:
    - Personal
    - Identifiable
    - Sensitive (healthcare/financial)
    - Information regarding minors
  - Identify the sources being used to collect the data:
    - Direct, explicit request from user (forms, surveys)
    - Analytics, behavior tracking
    - Third party data providers
    - Other sources of collected data…
  - Review how all personal information points are being utilized
  - Identify any outside parties with whom personal information points are being shared
- Overview of privacy controls
  - Review controls over the obtaining of data
    - Are the channels being used secure and/or encrypted
    - Identity confirmation and password protection (when relevant)
  - Review controls over storage of data
    - Encrypted storage
    - Secured from outside access
      - Digital access controls
      - Physical access controls
    - Internal access limited to appropriate parties through role-based access controls
    - Controls over retention length
      - Personal data should only be stored only as long as needed, and deleted/scrubbed/ anonymized when no longer necessary.
      - Sensitive data should be retained no longer than regulations allow.
  - Review controls over the processing/transmission of data
    - Encrypted transmission
    - Application security controls
    - Additional controls over 3rd party service providers
      Requirement of certification of security/privacy controls
      Requirement of non-disclosure agreement
  - Rights of data owners over their information
    - Confirm disclosure of data points being collected/stored
      - Confirm disclosure of how those data points are being used
      - Confirm disclosure of any outside parties with whom those data points are being shared
    - Confirm user ability to opt out of data collection
    - Confirm user control to request deletion of stored data
    - Confirm user process to redress errors in data
  - Review process for handling security breaches
    - Notification process
      - Law enforcement
      - Data owners
    - Investigation/Resolution process
    - Post-incident review and risk assessment
- Overview of privacy and data protection governance
  - Identify parties responsible for privacy controls and data protection
    - Information security governance
    - Risk assessment
    - Review of compliance requirements
    - Annual review of security measures
  - Review scope of privacy strategy
    - Department level effort
    - Corporate governance

APPENDIX A *(Continued)*

– Review evidence of strategy
  › Documented policies
  › Documented role responsibilities
  › Education and training of relevant employees on proper security principles and the importance of personal information security and privacy
  › Assessments, internal audits, or testing
    • Results documented, retained, and used for action planning

• Compliance with industry guidelines
  – Which are the guidelines to measure for compliance
  – How is compliance being promoted

ACCESS CONTROL

• Access control review
  – Review of procedures/policies for reasonableness
  – Access to application software, systems software, and sensitive data diligently controlled through passwords
  – Selection of user accounts from a sample of machines and processes
    › Verifying current access, the last update to account privileges, and the last time their password was changed
    › Validating that their current access is appropriate and consistent with policy
      • Obtain and review termination checklist to ensure that all necessary access revocations are being performed, and that these are tailored as needed for different roles/departments/management levels.
  – Verifying appropriate separation of roles and access between Development, Testing/QA, and Production environments
    › Confirm access controls over production data copied into development or QA environments.
      • Production data should be "cleansed" of all personal data when moved into non-production environments.
  – Verifying prevention, detection, reporting, and correction of unauthorized or irregular activities, both internal and external
    › How often are security logs checked?
    › Is automatic notification active? Who is contacted, and on what events?
    › Are any penetration tests performed internally or by external parties?
  – Confirm that reasonably up-to-date of security software are in place for both the local and application platforms, including malware protection, software patches, and virus definitions.
    › Confirm that procedures are in place to update and maintain all applicable security definitions and patches on a regular basis.
  – Hardware inventory control
    › Confirm use of an inventory of in-use and out-of-use hardware
    › Review maintenance for out-of-use data storage. Ensure that old storage devices are properly sanitized of critical data or destroyed.
  – Verifying physical access control to sensitive facilities (e.g. server room, data center, security center), policies, and logging

DISCLOSURES AND DEFINITIONS

• Status of required disclosures:
  – Privacy Policy
  – Terms of Service
  – Collected points of personal data
  – Usage of personal data and all sharing of data with third-party entities
  – Opt-out, deletion, and data correction options
  – Process for notification of data privacy breaches

About BPA Worldwide A not-for-profit organization since 1931, BPA Worldwide is governed by a tripartite board comprised of media owners, advertising agencies and advertisers. Headquartered in Shelton, Connecticut, USA, BPA has membership spanning more than 30 countries. Worldwide, BPA audits 2,600+ media properties—including business publications, consumer magazines, newspapers, web sites, events, email newsletters, databases, wireless and other advertiser-supported media—as well as 2,700 advertiser and agency members. Visit www.bpaww.com for the latest audit reports, membership information and publishing and advertising industry news.