APRIL 27, 2023

When Marketing & IT Don't Talk to Legal:

Minimizing Risk By Coordinating with Corporate Stakeholders

SHOOK
HARDY & BACON

ACC Association of Corporate Counsel
NORTHEAST

Presenters

Erin Leffler

Partner | Shook, Hardy & Bacon LLP
eleffler@shb.com

Kate Driscoll

VP of Compliance | Butterfly Network
kdriscoll@butterflynetinc.com

Alan Wong

Associate | Shook, Hardy & Bacon LLP
awong@shb.com

SHOOK
HARDY & BACON

ACC Association of Corporate Counsel
NORTHEAST

Privacy + Data Security

- Privacy and Cybersecurity Litigation
- Incident Response & Preparedness
- Privacy Compliance
- Proactive Risk Minimization & Thought Leadership

Agenda + Goals

- Website & Mobile App Advertising
- Cybersecurity
- Biometrics
- Privacy Compliance

Website + Mobile App Advertising

- What's the technology?
  - Session Replay
  - Pixels
  - Chatbots
  - Global Privacy Control (GPC) & Cookie Settings

Website + Mobile App Advertising

- Marketing
- IT / Website Development
- Legal

What's the Technology?

SESSION REPLAY

- Small pieces of code that replay a user's website visit
  - Improve user experience
  - Identify technical issues
  - Identify ways to improve conversion

PIXELS

- Piece of code that allows tracking of website visitor activities
  - Healthcare
  - Video Privacy Protection Act (VPPA)

What's the Technology?

CHATBOTS

- Programs built to automatically engage with consumer messages
  - Disclosure to consumers
  - Confidentiality / contract concerns

GPC & COOKIE SETTINGS

- Initiative to create global setting to allow user to control online privacy
  - Signal cookie preferences across websites

Legal Developments

- New application of wiretap laws
  - *Popa v. Harriet Carter Gifts* (3d Cir. 2022)
- Litigation trends – decisions on motions to dismiss
- U.S. Dept. of Health & Human Services
  - Office for Civil Rights (OCR) guidance (Dec. 2022)
- Federal Trade Commission enforcement
  - (BetterHelp)

Mitigation Measures

- Assess and understand your technology
- Maximize privacy controls
- Disclose your use of technology
- Consider the need for indemnification in contracts or a BAA with third parties
- Update policies and consent

Duty to Communicate

- Model Rule 1.4(a)(2)
  - "A lawyer shall …reasonably consult with the client about the means by which the client's objectives are to be accomplished."
- Model Rule 1.4(b)
  - "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."
- How to comply?
  - Keep client informed of technology advancements/developments that may assist in the provision of legal services.

Cybersecurity

- What’s the technology?
  - Secure backup processes
  - Endpoint detection & response
  - Records maintenance

Cybersecurity

- InfoTech
- InfoSec
- Legal

Legal Developments

- CCPA private right of action with statutory damages
- Rise of class action lawsuits
- Use of social media by plaintiff firms to identify clients
- Regulatory “walls of shame”

Mitigation Measures

- Third-party security assessment
- Document retention policy
- Faster response time to incidents

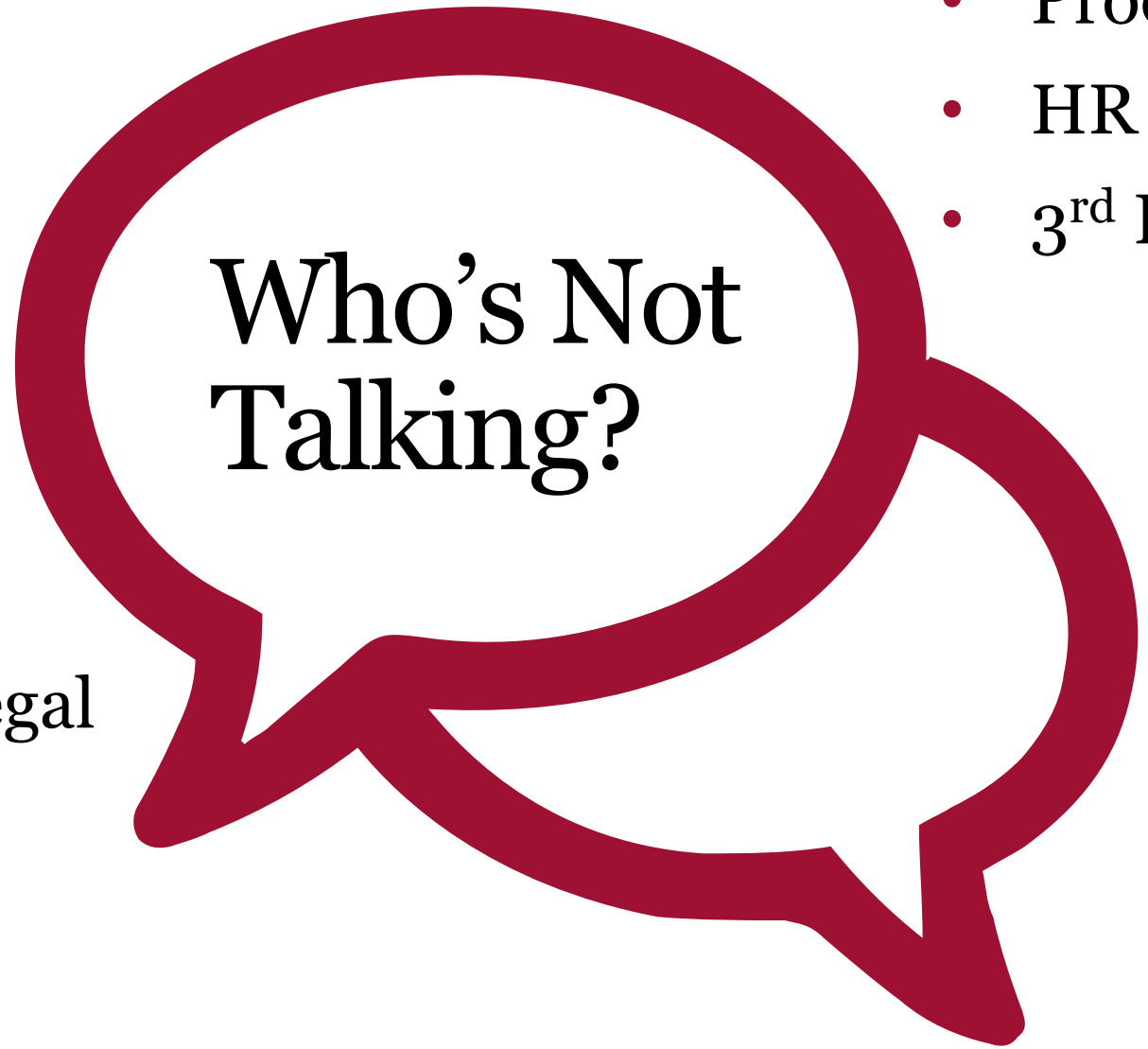
Duty of Confidentiality

- Model Rule 1.6(c)
  - "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."
- Comment 18 to Model Rule 1.6 lists non-exclusive factors to help lawyers in making the "reasonable efforts" determination, including:
  - The sensitivity of the information
  - The likelihood of disclosure if additional safeguards aren't employed
  - The cost of employing additional safeguards
  - The extent to which the safeguards adversely affect the lawyer's ability to represent clients
- How to comply?
  - Conduct a fact-specific inquiry to assess risks, identify and implement appropriate security measures, verify that they are effectively implemented, and ensure they are continually updated.

Biometrics

- What's the Technology?
  - Collection and use of biometric information
    - Timekeeping
    - Secure access to sensitive information

Biometrics



- Legal
- InfoSec
- Product
- HR
- 3rd Party Mgmt.

Legal Developments

- Biometric Information Privacy Act (BIPA
  - *Cothron v. White Castle Systems, Inc.* (Ill. 2023)
    - Separate violation for each scan or transmission
- *Tims v. Black Horse Carriers, Inc.* (Ill. 2023)
  - Five-year Statute of Limitations
- Update on Texas and Washington
  - "My Health My Data Act"
- Pending legislation in other states

Mitigation Measures

- Understand what you are collecting and why;
- Understand what biometric regulations apply to your business;
- Stay on top of technology changes;
- Conduct Privacy Impact Assessment - consider whether you need to collect biometric information
- Disclosures and consent from data subjects
- Train employees

Duty of Competence

- Model Rule 1.1
  - "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
- Comment 6 to Model Rule 1.1
  - "[A] lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…"
- How to comply?
  - "Lawyers need to understand basic features of relevant technology…For example, a lawyer would have difficulty providing competent legal services…without knowing how to use email or create an electronic document." *ABA Commission on Ethics 20/20*

Privacy Compliance

- What's the Technology and Business Practice?
  - Expansion of business into areas of the country & world
    - Different laws
    - More demanding privacy regulations

Privacy Compliance

- C-Suite
- Legal

Legal Developments

- California Consumer Privacy Act (CCPA)
- Other states following suit (Colorado, Connecticut, Virginia)
- General Data Protection Regulation (GDPR) and the UK
- Brazil (and the LGPD) & China (and the PIPL)

Mitigation Measures

- Understand expansion plans
- Understand the universe of data that is collected (customers, employees, third parties)

Organization as Client

- Model Rule 1.13(a)
  - “A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.”
- Comment 3 to Model Rule 1.1
  - “Decisions concerning policy and operations, including ones entailing serious risk, are not … in the lawyer's province.” When “the lawyer knows that the organization is likely to be substantially injured” by the action of a constituent that violates a lawyer’s legal obligation or “is in violation of the law” that may be imputed to the organization, the lawyer must proceed as “reasonably necessary” in the best interest of the organization.

State Ethics Opinions

- State Bar of Arizona, Opinion No. 05-04 (July 2005):
  - "an attorney must be competent to evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end. An attorney who lacks or cannot reasonably obtain that competence is ethically required to retain an expert consultant who does have such competence."
- State Bar of Arizona, Opinion No. 09-04 (December 2009):
  - "technology advances may make certain protective measures obsolete over time… As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information."
- State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179 (2010):
  - "In accordance with the duties of confidentiality and competence, an attorney should consider the following before using a specific technology:
    - a) The attorney's ability to assess the level of security afforded by the technology…
    - b) Legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person's electronic information… [and]
    - c) The degree of sensitivity of the information[.]"

State Ethics Opinions

- New Jersey Advisory Committee on Professional Ethics, Opinion 701 (April 2006):
  - "The critical requirement under RPC 1.6, therefore, is that the attorney exercise reasonable care against the possibility of unauthorized access to client information… What the term reasonable care means in a particular context is not capable of sweeping characterizations or broad pronouncements. But it certainly may be informed by the technology reasonably available at the time to secure data against unintentional disclosure. Obviously, in this area, changes in technology occur at a rapid pace."
- New York State Bar Association Ethics Opinion 1019 (August 2014):
  - "A law firm may use a system that allows its lawyers to access the firm's document system remotely, as long as it takes reasonable steps to ensure that confidentiality of information is maintained. Because of the fact-specific and evolving nature of both technology and cyber risks, this Committee cannot recommend particular steps that constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients."
- New York Bar Association Committee on Professional Ethics Opinion 842 (September 2010):
  - "A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality is maintained… In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information[.]

Questions?

SHOOK
HARDY & BACON

ACC Association of Corporate Counsel
NORTHEAST