Conducting a Privacy Audit

A regulatory compliance approach or performance improvement ?

Ruth V. Nelson

PricewaterhouseCoopers Privacy Practice

www.pwcglobal.com/privacy

Elizabeth B. Carder, Esq.

Reed Smith LLP

Washington, DC

The First National HIPAA Summit

You have already heard

- Overview of HIPAA: implementation & enforcement
- Privacy Officer Roles and responsibilities, & coordination strategies
- Compliance Tools, eSignatures & International Rules
- Ethics & Details of the Rules

And now an approach to determining if you are getting it right..

Why are we here?

"Most people don't do what they believe in . . . They do what's most convenient and then they repent."

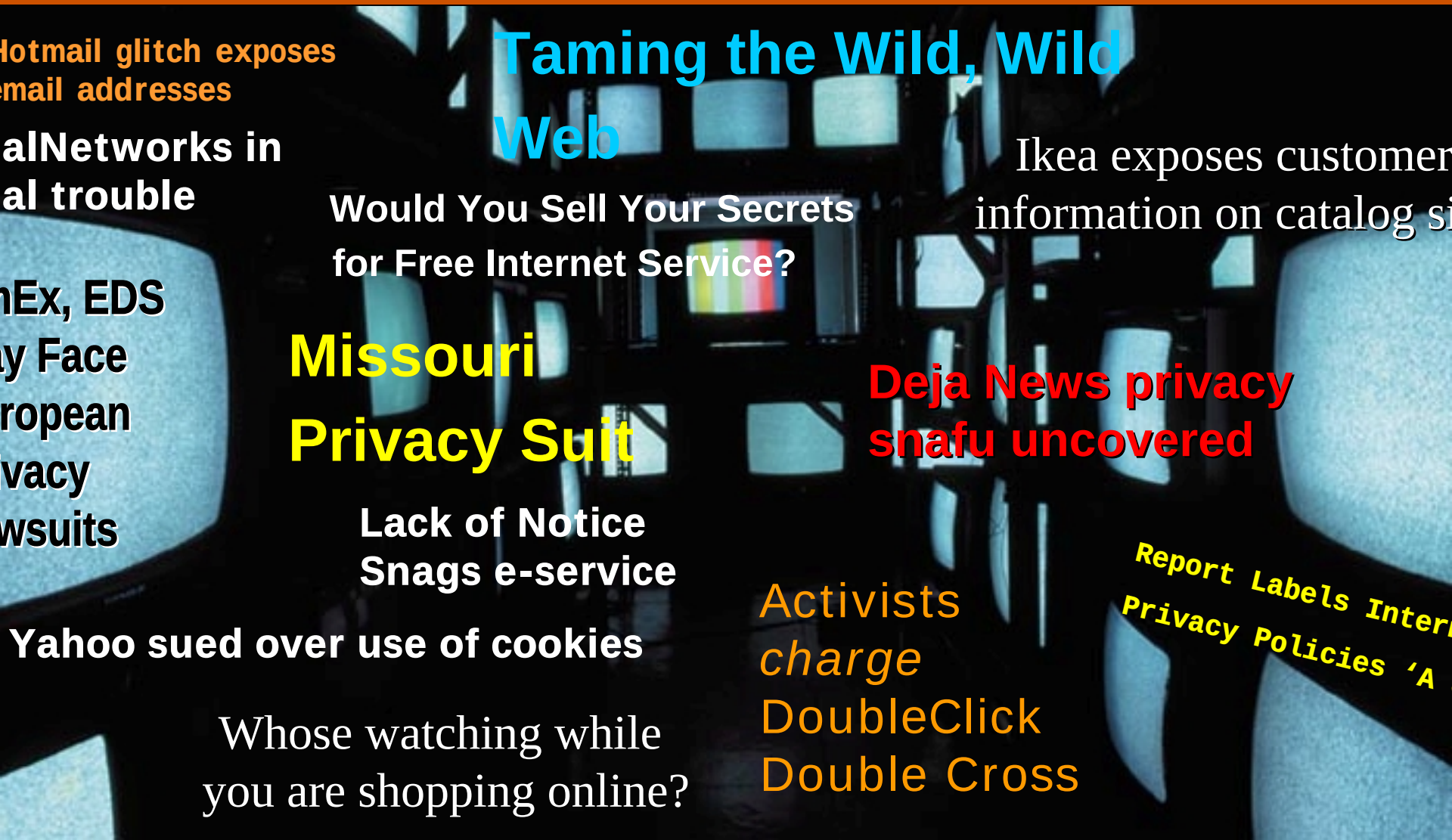
Quote: Bob Dylan

Making it convenient means . . .

To have privacy practices that do not diminish the economic viability or integrity of the healthcare industry. The key is to do this in such a way as to not violate the range of new regulations and growing public concerns.

Where does your organizational culture fit ?

- Repent or Proactive



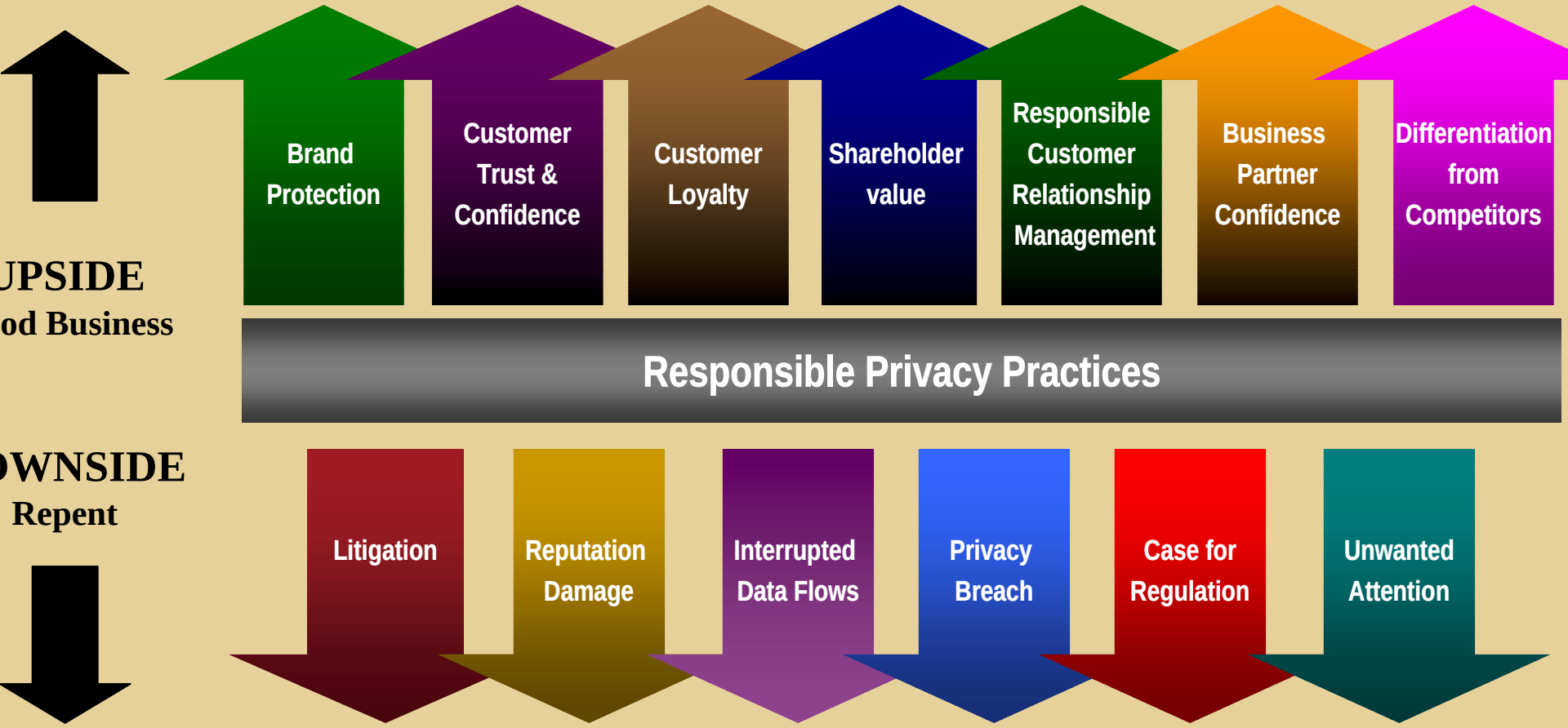
What If ? ……..

Privacy is not just another compliance requirement...

...but a key way to differentiate and market your business

So that….Privacy is just good business

The Full Impact of Privacy - its just good business



ay's Process:

Manually intensive

Reactive to crisis

Not core to business

Difficult to easure and monitor

he Future:

b Enabled ompliance

Privacy Audits and Trust

“Trust” in the Privacy Space

Transparency:

- Provides openness and clarity to all activities concerning the capture, collection, dissemination and use of consumer data

Stewardship:

- Assumes a “fiduciary responsibility” over the handling and protection of consumer information (irrespective of the source of this data)

Proposition . . .

Beyond good security and privacy policies, transparency requires proof of proactive compliance.

Independent verification or “audit” is a practical solution for determining the quality and integrity of privacy practices and enhancing transparency.

Preparing for a Self-Audit - Today plus one year !

- You have Mobilized the Privacy Officer and Task Force
  - connected to external resources, POA, P&AB's CPO
- Legal counsel has a litigation prevention strategy in place
- You know your dataflows, information-handling practices and third party chains of trust
- You have integrated HIPAA Privacy Compliance with other Privacy Rules - GLBA, Online Privacy, Safe Harbor, Hi-Ethics Principles….
- You have determined your "go to" compliance business processes and begun implementation
- You have implemented new training via e-learning

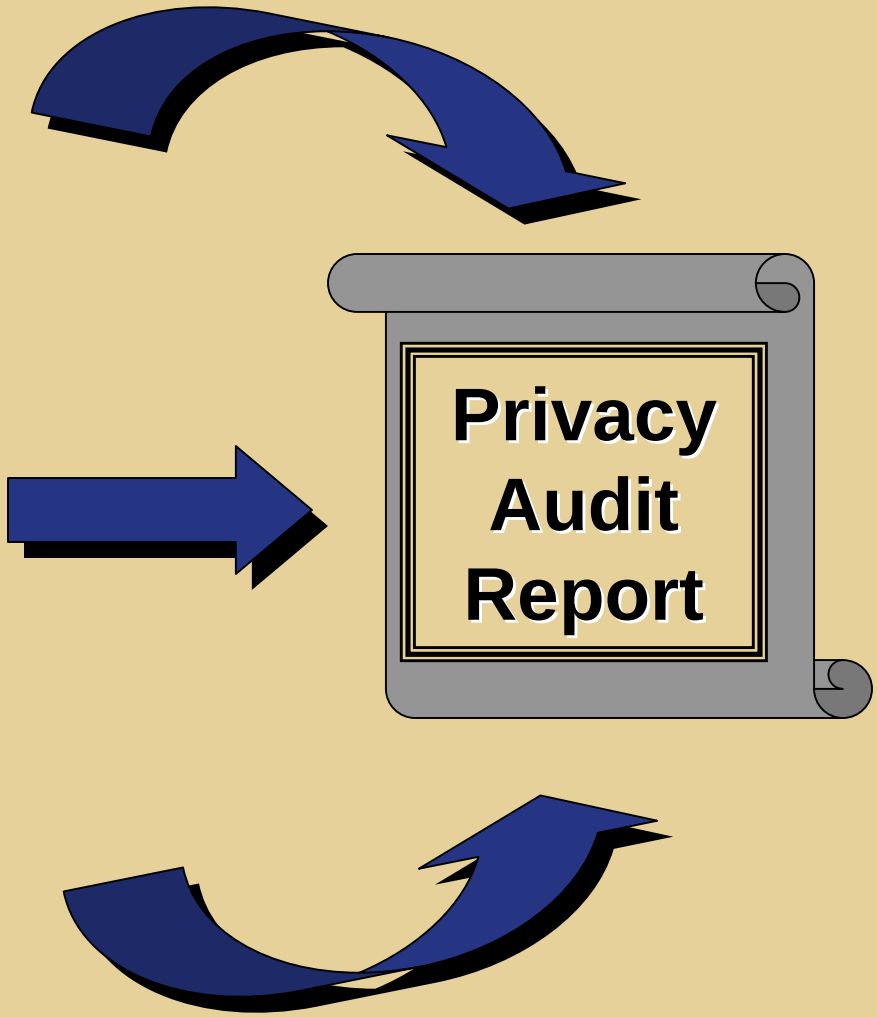
About the Privacy Audit

The General Privacy Audit

Should reflect privacy best practices or generally accepted industry standards

Must have sufficient control systems and technology backbone to secure standards

Must accurately reflect business practices, with strict quality standards for the auditor



Different Levels of “Assurance”

- Following are different forms of assurance options as a means to engender consumer trust
  - Privacy ratings
  - Seal programs
  - Independent Audit
  - Governmental Audit

Scope of the Privacy Audit

- The Company
- Business partners
- Technology partners
- Business customers/merchants & the chains of trust
- Final consumer

Nature of the Privacy Audit

- **The privacy audit deals with three levels of compliance, as follows:**
  - **On Existence** - does a privacy policy and related compliance program exist?
  - **On Coverage** - does the privacy compliance program apply to all relevant areas of business practice?
  - **On Effectiveness** - does the privacy compliance program meet or exceed stated goals?

The Audit Report

- **Nature of the report** -- What does it say?
- **Frequency of the report** -- How often is it presented
- **Circulation of the report** -- Who gets to read it?

Are actions derived from the audit that feedback into performance improvement of the compliance business processes ?

Considerations for Quality Results

- Above the “bar” assertions
- Objective audit criteria - based on accepted industry standards
- Full scope of work - including effectiveness of compliance business processes, preventative vs detective controls
- Frequency of the audit
- Enforcement
- Incident Management and reviews
- Quality controls and peer review process
- Dispute resolution process

New Audit Models

- Real-time Auditing
  - Technology Agents embedded in your networks, that automatically flag items of concern, eg customer database extracts outside of automated and secure scripts, seeding of consumer opt-outs
- Audit enabled compliance processes
  - using company-wide compliance systems that have built-in actions and compliance requirements with verifiable audit trails
  eg legal counsel flags a new type of third party arrangement as part of a chain of trust, CPO required to review and sign-off compliance
- Privacy Enhancing Technologies
  - For web based loyalty strategies, self-managed records
- eSignatures - digital certificate authentication

Aggressive advocates, new laws and regulations in this area make it difficult to “conveniently” avoid taking action in the privacy arena.

The chance for proactive leadership in the industry is now.

Next Steps ...

- Support compliance with proactive privacy practices and systems-enabled design
- Use advanced technologies to connect, authenticate and protect your systems and consumer data
- Validate your privacy compliance strategy through independent verification via a privacy audit
- Manage privacy compliance through effective tools such as e-compliance solutions

Questions

Ruth V. Nelson
Privacy Practice
PricewaterhouseCoopers
(202) 414-1463
ruth.v.nelson@us.pwcglobal.com

Elizabeth B. Carder, Esq
Reed Smith LLP
Washington, DC
(202) 414-9210
ecarder@reedsmith.com