Of Skunks & Canaries (and maybe rat holes)

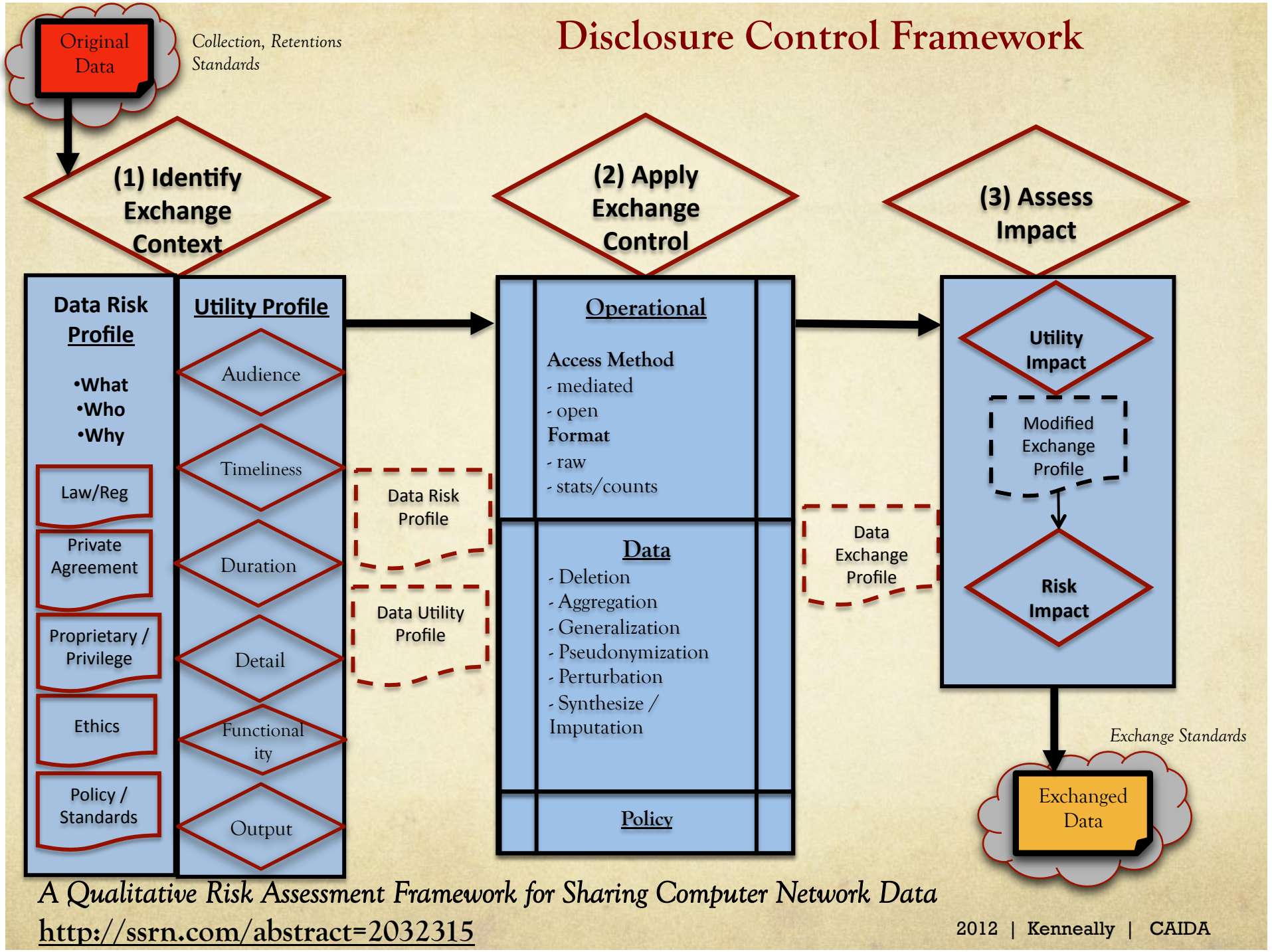
Workshop on Internet Economics
Dec 2012
Erin Kenneally, CAIDA

Reality of Network Data Sharing

- Uncertainty of legal risk
- Understated value of potential benefits
- One-size-fits-all approach to disclosure controls
- Implicit assumption that any sharing increases risk
- Results in:
  - Data rich vs. data poor
  - Sharing through ad-hoc, interpersonal relationships
  - Scarcity of scalable, transparent, sustainable sharing

Data Exchange Risk-Utility Approach

- Qualitative framework for:
  1. Identifying specific utility goals and related risks
  2. Choosing disclosure controls to address risks
  3. Assessing effects of those controls
- Generalizable across all network data & scenarios
- Enable data providers to:
  - Better understand sources of risk
  - Tailor controls to intended utility
  - Justify choices and explicitly state assumptions
- Promote the social value of shared data & process



A Qualitative Risk Assessment Framework for Sharing Computer Network Data

http://ssrn.com/abstract=2032315

2012 | Kenneally | CAIDA

Enter the

Tweet Permalink

Patient Data Breaches: Future Looks Grim

Inadequate security funding, tools and expertise could cost healthcare industry billions of dollars annually, finds Ponemon/ID Expert's third annual study.

By **Michelle McNickle** InformationWeek
December 06, 2012 02:06 PM

A majority of organizations polled for Ponemon and ID Expert's third annual benchmark study on privacy and security don't have the technologies, resources and trained personnel in place to take on modern-day privacy and data security risks.

Since beginning the benchmarking in 2010, Ponemon and ID Experts have found that threats to healthcare organizations have increased. The organizational costs for dealing with breaches are climbing as well, with the average price tag increasing from $2.1 million in 2010 to $2.4 million in 2012. The report projects that eventually the annual cost of continuous breaches for the industry "could potentially be as high as $7 billion."

Entering the Mine?

- Context: Architecture, Innovation, Governance Relationship Model
  - Do we need regulation? Will self-reg/market approach work
- Internet Privacy - how has industry self-reg fared?
  - Data opacity; Info asymmetry; Identity bundling
  - Similar celebrity death matches: Indiv and collective consumer privacy v. Industry innovation, security, anti-fraud
  - Many terms not defined (e.g., innovation, harm & threshold)
  - How does/will de-reg impact consumers? Systemic risk? Industry goals met?
  - Measurement--provocateur dynamic

: Way Down the Well?

Objective → B.C. → A.D. → Post-Op

* Individual Privacy * Increased Security → Decreased Systemic Risk	* Breach stat free 4 all * Detection, flipping kimono, shaming	* Breach fatigue * Open admission of overwhelm * Breaches normalized	*Institutionalizd problem to support sustainable biz model? *Objective met??

Data Breach Disclosure Laws

* Decreased Systemic Risk	* Net stat free 4 all * Shenanigan shaming	* Discrimination fatigue *Normalize actions as function of market demand to innovate	*Institutionalizd problem to support sustainable biz model? *Better networks??

Private Network Disclosure Mandates … same trajectory?

"Every great cause begins as a movement, becomes a business, and [most] eventually degenerates into a racket"