Data Exchange Policy: Avoiding the Zero-Sum Trap

Erin Kenneally

Elchemy

U. California San Diego, CAIDA

Not another talk on data sharing!

- **Avoiding Groundhog Day–**
  - Conceptual framing : how we got here, how to advance policy
  - Operational framing : Strategic Policy Data Exchange

- **ENISA, Council of Europe new workgroup**-
  - late Nov '12, Turkey, ~14 nations
  - promoting international data exchange standards/guidance
  - to update legislation and clarify legal muddiness re: privacy and data protection
  - to harmonize with industry, NGO first responders data wealth and scale utility
  - Win-win: cyber security and counter e-crime
- **Octopus Conference on Cybercrime**
  - June 2012, Strasbourg
  - focus on public-private info exchange, cybercrime legislation and transborder access to data.
- **U.S. legislative activity**- comprehensive cyber security bill

- **History**: Budapest Convention –
  - first intl treaty on crimes committed via the Internet/networks (2001)
  - Harmonize substantive crim law; procedural law for LE; cooperation regime
  - Belgium 9/12 ratify = 37

← The Cloud: Private as Curbside Garbage?

History as Innovation: The Intellectual Legacy of Eric Hobsbawm →

A U.N. Takeover of the Internet: Existential Threat or Tempest in a Teapot?

Posted on August 9, 2012 by Zachary Tumin

Experts disagree whether an upcoming meeting of the International Telecommunications Union in Dubai will determine the future of global Internet governance.

By Jonah Force Hill

On Thursday, May 31, 2012, in the Rayburn Office Building of the House of Representatives, a panel comprising some of America's leading Internet industry and policy experts offered an ominous warning to U.S. lawmakers about future of the Internet.

"The open Internet has never been at higher risk than it is now," testified Vint Cerf, one of the 'fathers of the Internet' and Google's self-described "Chief Internet Evangelist." "A new international battle is brewing," he asserted, "a battle that will determine the future of the Internet."

he Pentagon, but the Defense Department's latest endeavor putting aside billions to enhance its cyberwar capabilities.

Agency, DARPA, is turning towards the private sector and it forces for its next war. A report released Thursday by the t $1.54 billion during the next five years to up its online bbed Plan X, but unlike before it won't be budgeted the Pentagon is itching to ensure that America can carry out an dying the US to defend itself against a similar assault from

Reading Policy Tea Leaves

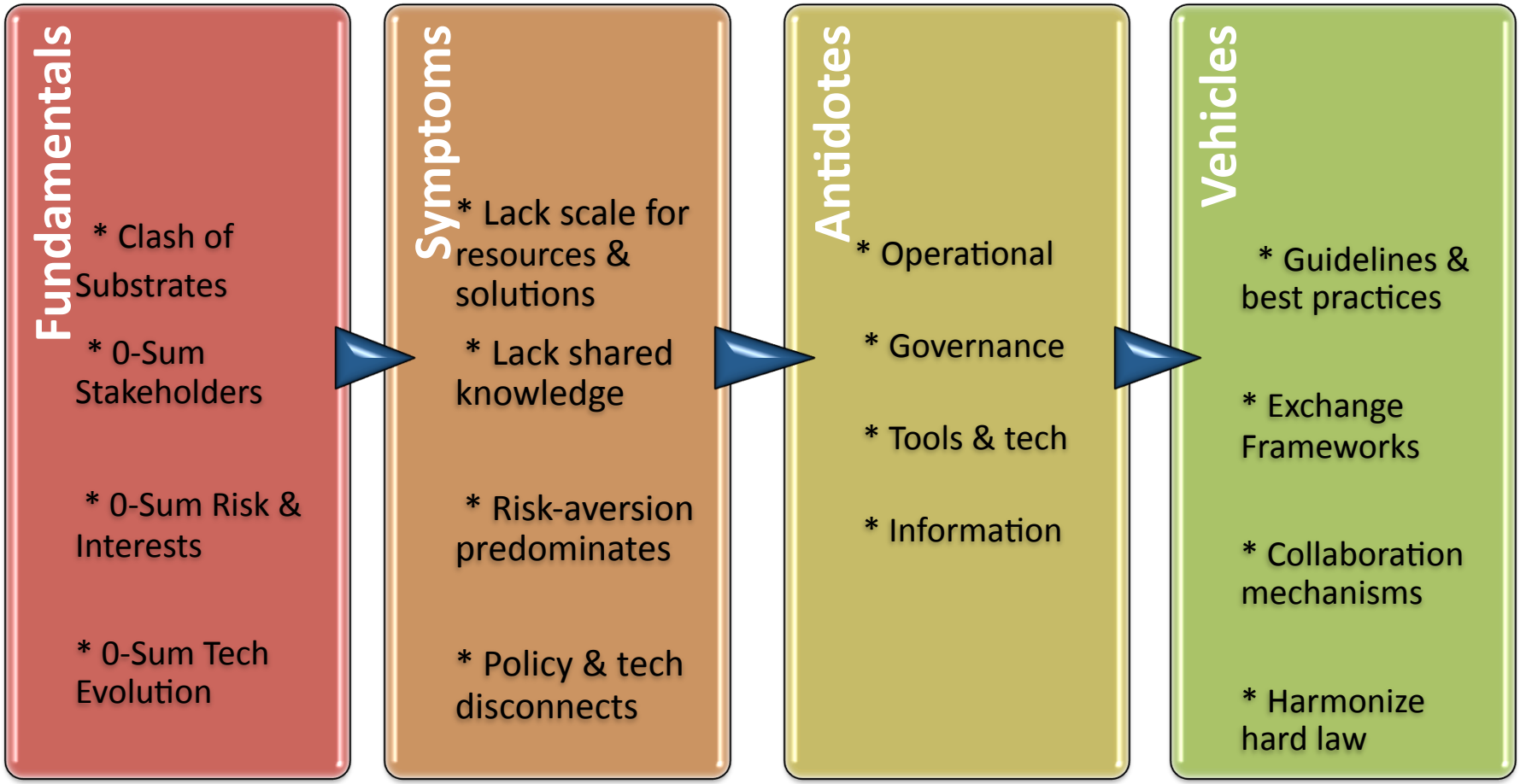
- H.R. 3523, **Cyber Intelligence Sharing and Protection Act (CISPA)** (Rogers-Ruppersberger)
  - procedures allowing intel cmmty to share cyber threat intelligence with private-sector
  - a cyber-security provider or a self-protected entity may share "cyber threat information" "with any other entity designated by such protected entity, including… the Federal Government."
- S. 3414, **Cybersecurity Act** of 2012 (Lieberman-Collins-Feinstein)
- S. 3342, **SECURE IT Act** of 2012 (McCain)
- **Hoorah! …**
  - What info may be shared
  - Who may receive cybersecurity related info
  - How may info be used, redistributed
- **Or, not …**
  - Opposed by 'web users': lack clarity about meaning of terms (breadth) and how implemented
  - Big Industry (Internet & telcos) support
  - EoP opposes; supports DHS lead
  - Would liability shield actually impede cyber security?
  - End run around privacy, civil liberties, confidentiality (e.g., ECPA)

Reality of 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
- * **Solutions** are **Tactical** policy & technical implementation

- **Perpetuates**:
  - Data rich vs. data poor
  - Sharing through ad-hoc, interpersonal relationships
  - Scarcity of scalable, transparent, sustainable sharing
  - * Solutions are **not SP-SVR = Strategic Policy-Shared Values and Resources**

Advancing Strategic Policy-Shared Values & Resources



ALCHEMY®

(1) Fundamentals of Data Exchange Issues

Clash of the Substrates: values, processes and resources

- **Internet: Shared global ownership** – decentralized
  - Values and resources - collaborative researchers, industry, civil society, government
  - Processes for tech & policy development – transparent & freely accessible
  - Governance – expertise & collaborative multi-stakeholder driven

- **Law and biz models : 0-sum between stakeholders**
  - 2-D (bilateral, linear) stakeholder model: individual (person, org) rights and obligations-centric
  - stages rights holders conflicts
    - today's problems involve multilateral conflicts, ecosytem contexts (threats not time/space bound)
    - security v. cybercrime enforcement v. privacy v. innovation/cost v. natl security v. IP protection
    - netflow records- do individuals have privacy rts in the aggregate? Does industry have right to innovate from? Does gov't have right to surveil for natl security? YES and NO
  - so, rts and obligations born individually, not collective/multilaterally

- **Law and biz models : 0-sum between risk and benefits**
  - Proscriptive → risk aversion… not so much prescriptive → benefit
  - Inversely proportional: industry risk (data protection obligations, network data disclosure prohibitions) inures to individual benefits/utility (elec comm privacy) and to the detriment of societal utility (counter e-crime) and industry utility (innovation)

- **Law and biz models : 0-sum with technology evolution**
  - inconsistent/silent about risks, intermediaries not neutral?
  - eg, cloud computing - DE sharing, applying data protection standards

(2) Symptoms

- Lack of scale - resources and exchange solutions
- Lack of shared skills and knowledge/understanding between stakeholders
- Easy to stonewall, risk wins (easy for risk manager to say “no”)

(2) Symptoms

- Disconnect between policy and technology
  - Lack of legal precedent or guidance for network data risks:
  - Data complexity (heterogeneous, volume, variety of actors) … Not just PII

  - Difficulty bounding attack risk
    - Cannot quantify access to secondary data sources
    - Privacy definitions are immature for network data
    - eg, Article 29 Data Protection Working Party (10/5/12)
      Suggest changing Def of "personal data".. identification numbers, location data, online identifiers or other specific factors as such should as a rule be considered [*delete:need not necessarily be considered as*] personal data [*delete: in all circumstances*].'

(3) Antidote/Cure

Stress social values (shared resources) and social risks

- **Operational & Governance**:
  - clarify uses by recipient
  - define workflow, policies & procedures that negatively affect DX
  - common reporting standard
  - understanding role and parameters for co-operation

- **Tools and Tech** : knowledge and case management systems, secure comm channels
- **Information** : structure, content, use, level of detail, exchange standards

(4) Delivery Vehicles-
How Might APWG Steer/Sit Shotgun?

- **Guidelines/Best Practices/Checklists**
  - In the language and terminology of the stakeholders (e.g., LEA working w/ CERTS)
  - procedures and capabilities
  - assessing, responding, submitting requests for different data (human-application layer, device layer)

- **Risk-Utility Exchange Framework**
  - standardized approaches for dealing with legal challenges
- **Collaboration mechanisms** : unstructured/informal, collab forums, joint exercises, structured/formal comms, co-produced materials, joint training, common workflows, trust consortia (CSIRT, FIRST, APWG)

- Inform legal liaisons; change/**harmonize hard law**

/E.g./ Strategic Policy Exchange Framework

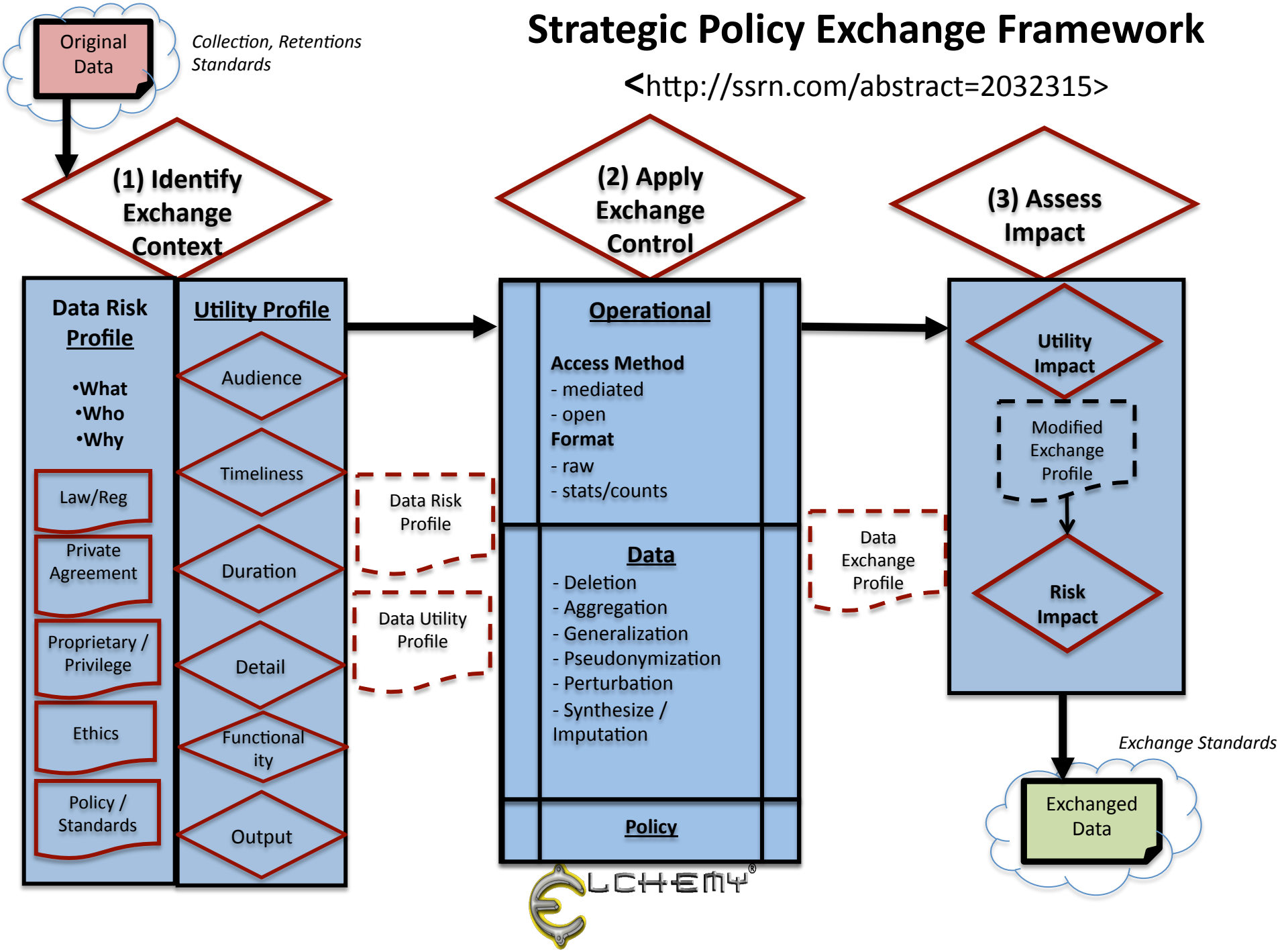
- **Qualitative framework for:**
  1. Identifying specific utility goals and related risks
  2. Choosing disclosure controls to address risks
  3. Assessing effects of those controls
- **Generalizable** across all network data & scenarios
- **Enable data providers to**:
  - Better understand sources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

- Promote the **social value of shared data & process**

ECHEMY®

Strategic Policy Exchange Framework

<http://ssrn.com/abstract=2032315>



SP Exchange Framework Value for Stakeholders

- **Data Exchange Profile Templates** that embed different:
  - Definitions of cybercrime/incident/attack
  - Rules on DE, privacy and data protection, data retention
  - Knowledge of own and other S's rules
  - Information and flow- evidence v. intelligence, give & receive
  - Charters and objectives
  - Capabilities

Transcending 0-sum Data Exchange

- Find **common-ground** around these notions:
  - ≠ widget world: data exchange must change/fit biz process
  - ≠ one-night stand: data exchange longer-term mentality
  - = operationalizing Strategic Policy of Shared Values & Resources
- Next stop: Istanbul whitepaper… input sought & welcome

Thank-You!

Erin Kenneally
erin@elchemy.org

ELCHEMY®