Data Protection Futures: Empowering the Right of Privacy - Informational Self-Determination

Kevin O'Neil

CYVA Research Corporation

koneil@cyva.com

Thursday April 17, 2008
Health Information Privacy and Security Awareness Week

Data Protection Futures

Agenda

- Forces Shaping Data Protection
  - Multifaceted Challenges of Human-digital Existence
  - Battle for Control of Personal Information
  - Data Slave Trade: Reality Check
  - Paradigm Shift and Consequences
- Potential Data Protection Futures
  - Identity Management – User-centric v. Corporate-centric
  - Experimental Technology: Personal Information Agent
  - Privacy Frameworks & Architectures
- Recommendations & Questions

Papers

Securing and Asserting the Mutual Rights & Responsibilities of Human-digital Existence: Informational self-determination

Self-determining Digital Persona: Empowering Citizen-centric Command & Control of Digital Identity and Information Assets, Anywhere, Anytime

CYVA Research Corporation

Papers

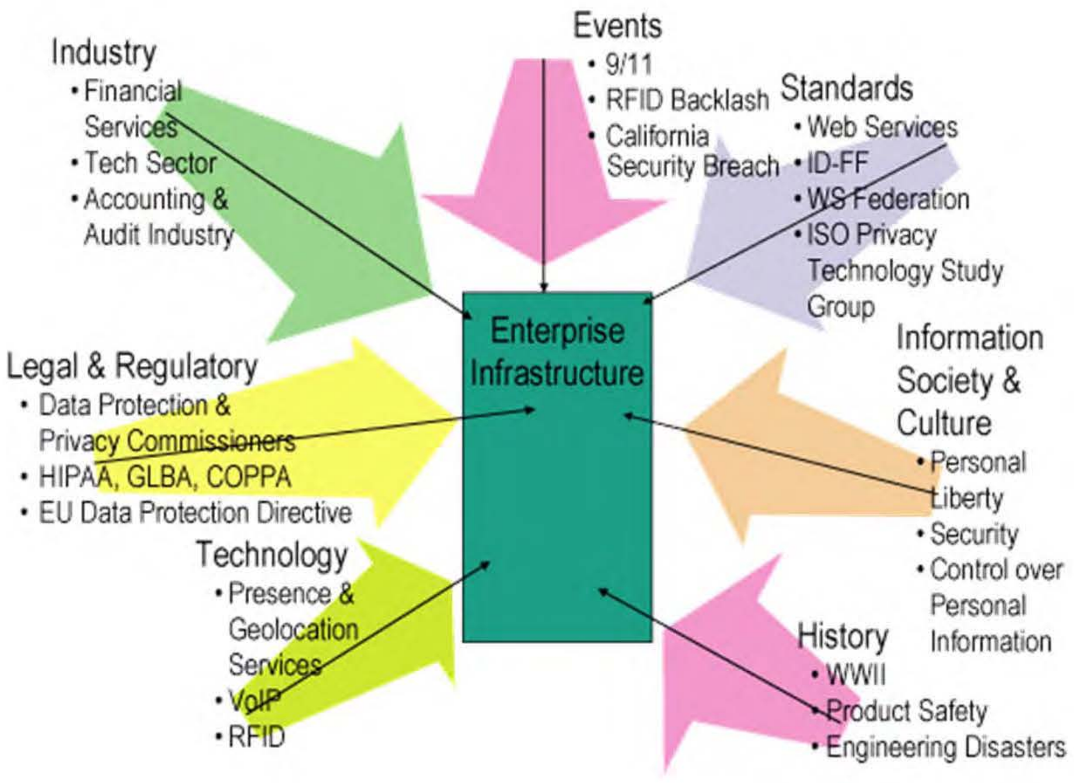
Data Slave Trade

An Argument for the Abolition of Digital Slavery: The Intrusive & Coercive Collection and Trafficking Of Personal Information for Profit and Power

For a Better Union of Social, Economic and Political Liberty, Justice and Prosperity Recognize and Secure the Mutual Rights & Responsibilities of Human-digital Existence

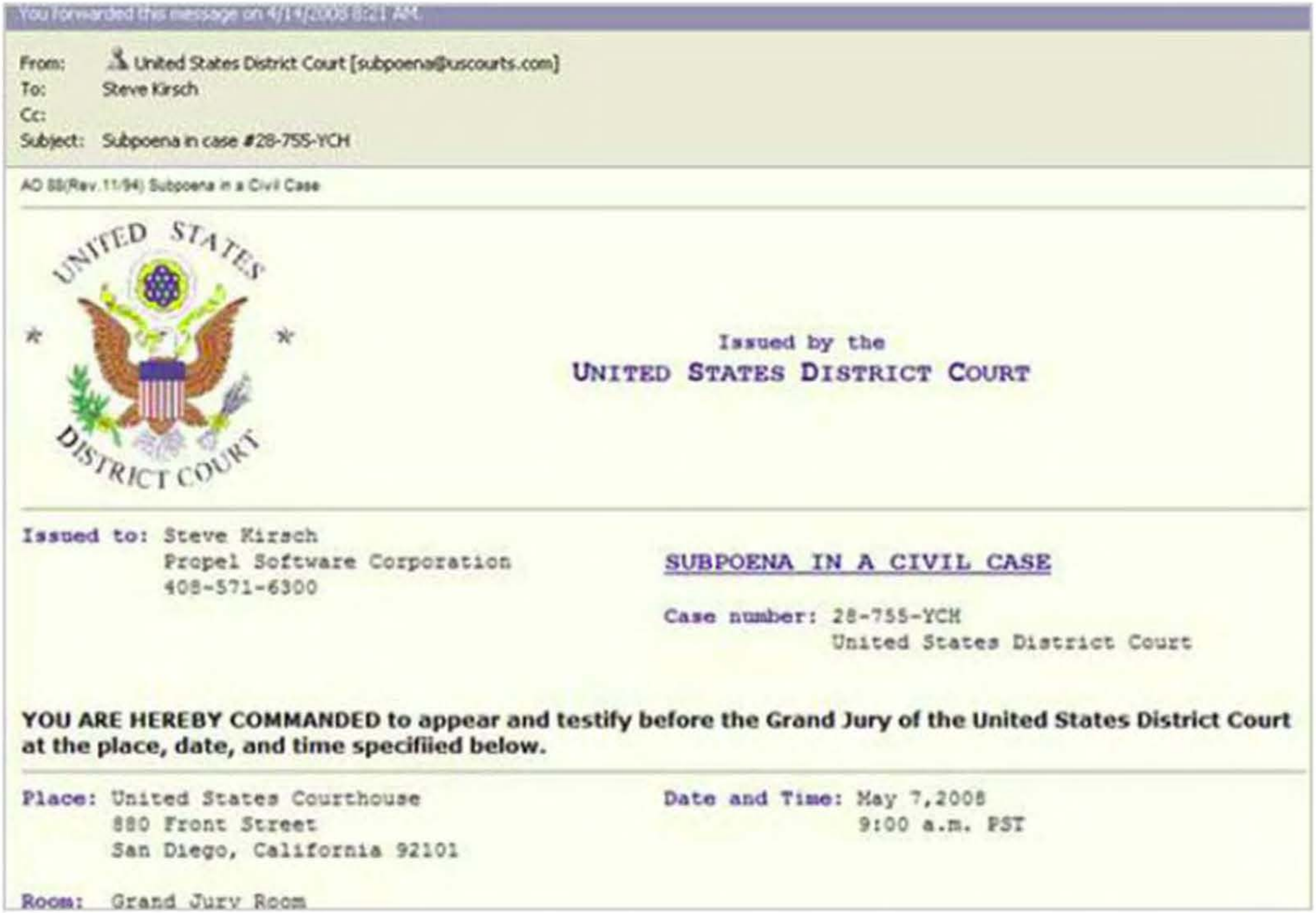
CYVA Research Corporation

Analysis: Forces Shaping Data Protection


Industry
• Financial Services
• Tech Sector
• Accounting & Audit Industry
Events
• 9/11
• RFID Backlash
• California Security Breach
Standards
• Web Services
• ID-FF
• WS Federation
• ISO Privacy Technology Study Group
Enterprise Infrastructure
Legal & Regulatory
• Data Protection & Privacy Commissioners
• HIPAA, GLBA, COPPA
• EU Data Protection Directive
Information Society & Culture
• Personal Liberty
• Security
• Control over Personal Information
Technology
• Presence & Geolocation Services
• VoIP
• RFID
History
• WWII
• Product Safety
• Engineering Disasters

Whaling

The New York Times April 16, 2008



You forwarded this message on 4/14/2008 8:21 AM.

From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev.11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specifiied below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

An image of the fake document contained in e-mail messages sent to thousands of executives as part of an online scam.

MySpace Has No Solution

TIME

Time Magazine, July 3, 2006
How Safe is MySpace?

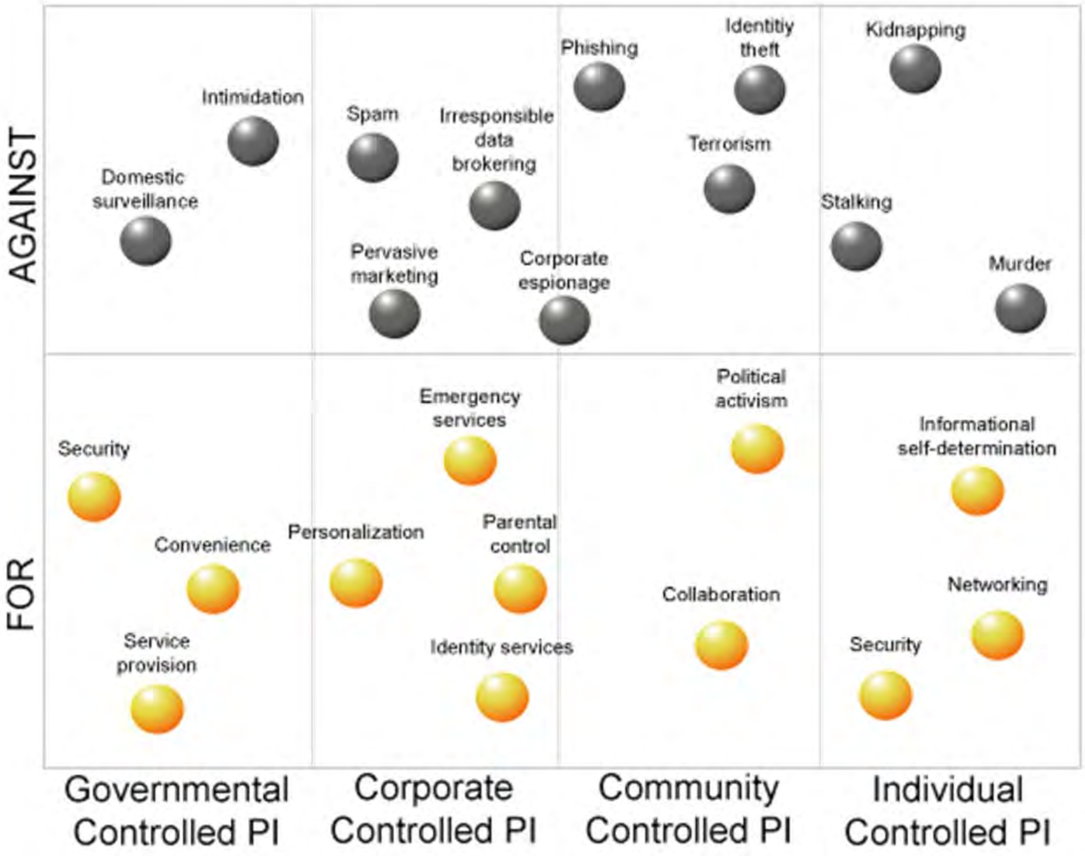
“There is no technology or national system that exists that allows us or any Internet company to verify the identity of people online.”

Hemanshu Nigan, Chief Security Officer for MySpace

Resistant and Irresponsible Corporate Behavior:
Parents are livid and seeking solutions

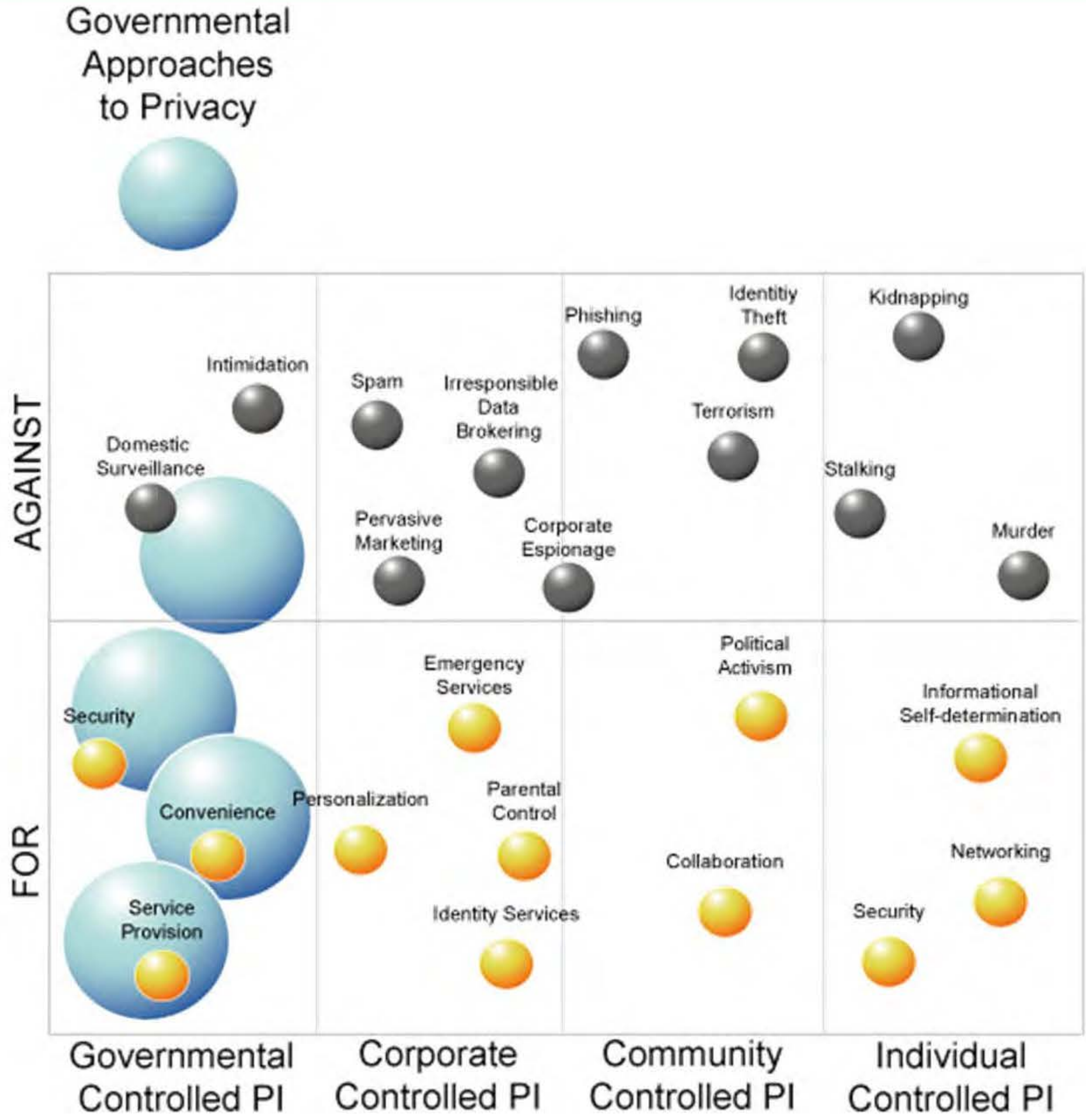
Analysis: Competition for Control

“CEO Eric Schmidt admits that Google ads on mobile phones will be more than twice as profitable as Web ads because of hyper-personalization and targeting.”

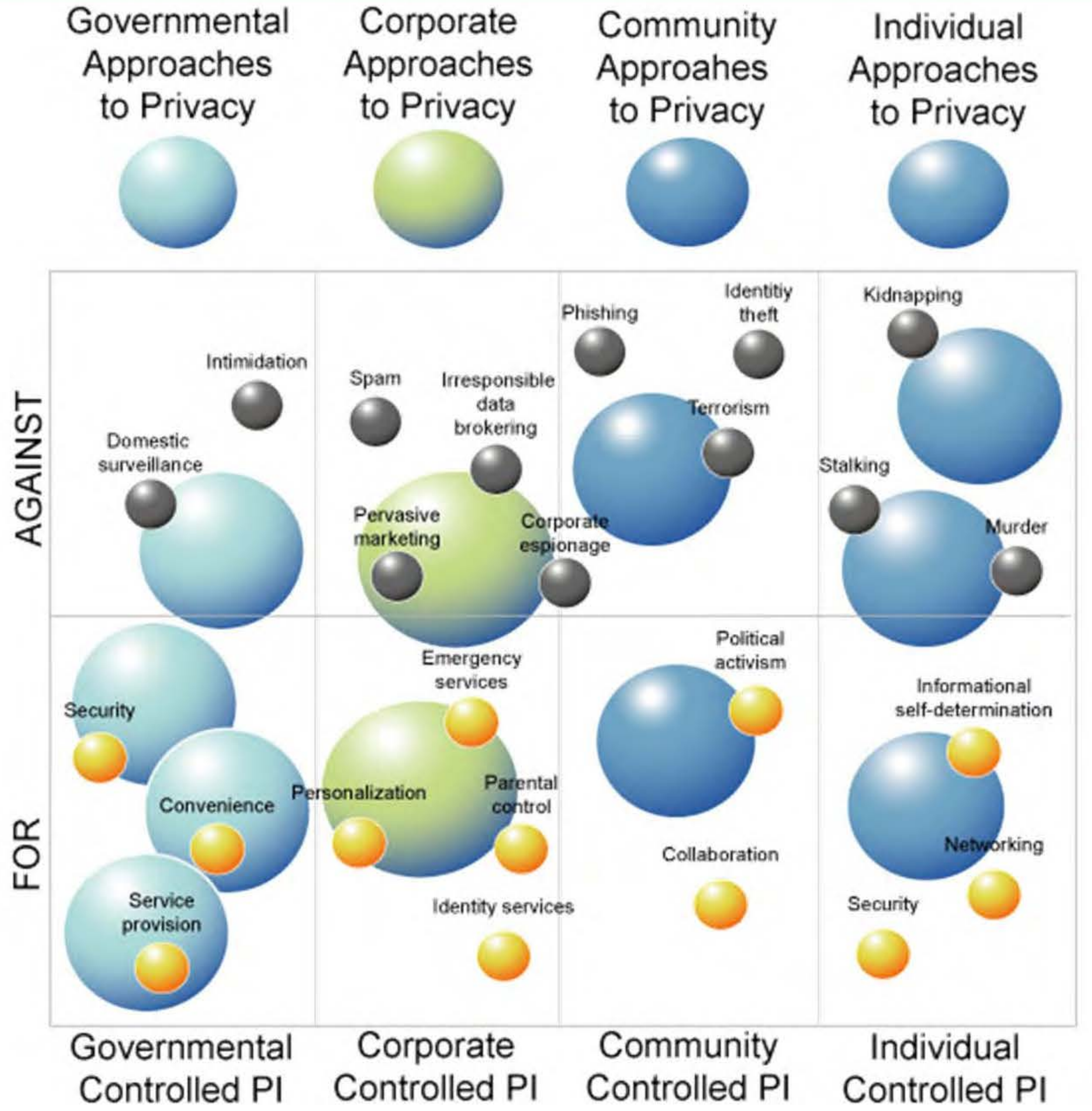


	Governmental Controlled PI	Corporate Controlled PI	Community Controlled PI	Individual Controlled PI
AGAINST	Intimidation Domestic surveillance	Spam Irresponsible data brokering Pervasive marketing	Phishing Identitiy theft Terrorism Corporate espionage	Kidnapping Stalking Murder
FOR	Security Convenience Service provision	Emergency services Personalization Parental control Identity services	Political activism Collaboration	Informational self-determination Networking Security

Analysis: Competition for Control



Analysis: Competition for Control



Paradigm Shift: Human-digital Existence

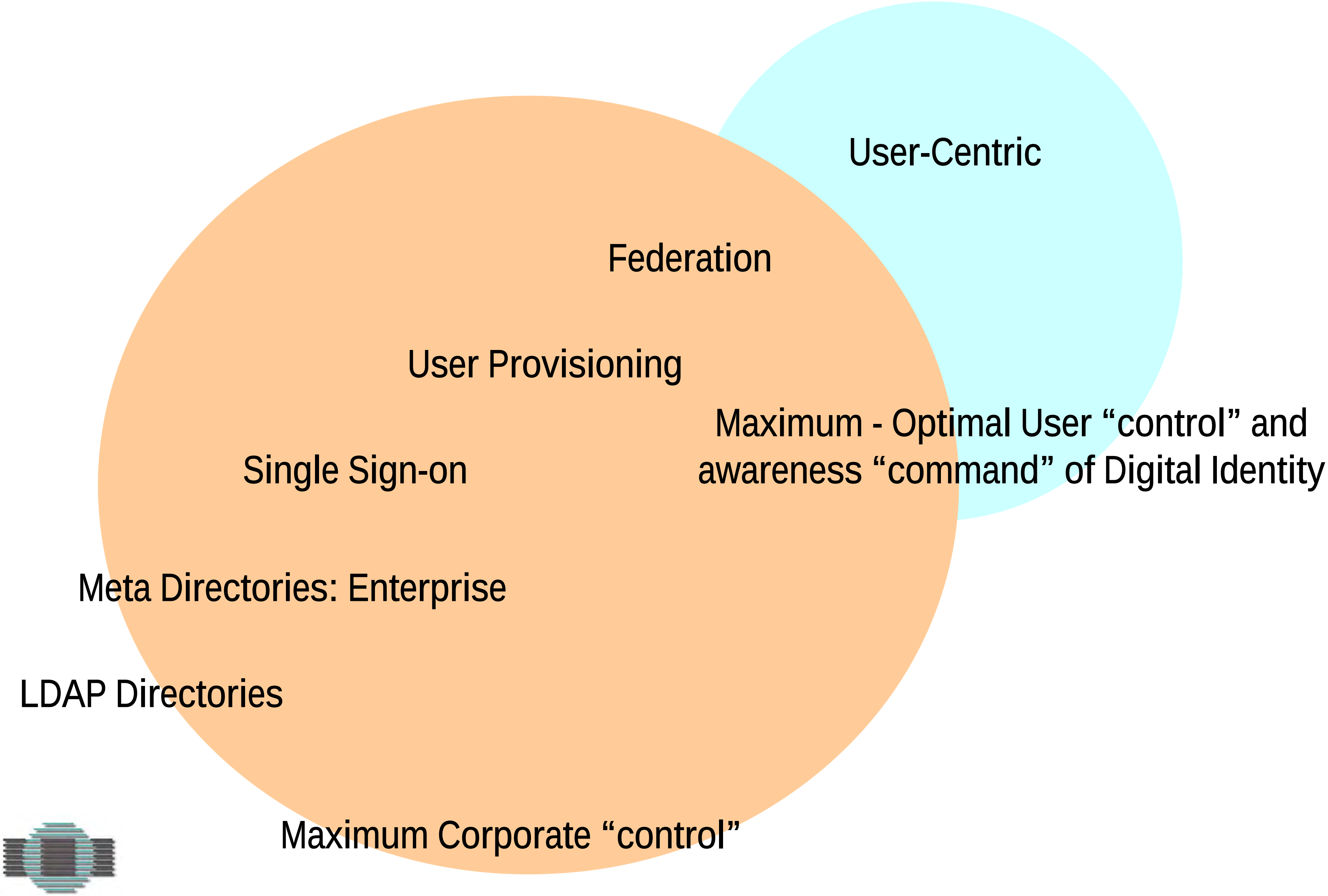
Paradigm shift

- The causal relationships between our logical and physical existence are more apparent each day.
- The dignity of man is being translated into the dignity of digital being.
- I am data. I have rights. Treat me (Digital Being) with respect or else is not an idea and attitude to be ignored or discounted.
- Assertive privacy technology will overshadow passive privacy enhancing technologies. The ability for consumer-citizens to securely command and control their personal information will act as a catalyst for a new order and arrangement.
- Infomediaries and information-for-value or benefit transactions are not out of the realm of serious strategic consideration and assessment today. Data gathers see the inevitability of a privacy paradigm shift, an end to business as usual.

Data Slave Trade

- Transatlantic Slave Trade Then
- Today we as human-digital beings are:
  - Denied our dignity and existence as equal and free human-digital beings
  - Callously and intentionally denied our human right of informational self-determination
- Captured, chained, branded and declared property of others
- Forced into unending labor and exploitation for the profit and power of others
  - Denied just compensation for the use of our identity and information assets
  - Denied the power to control our digital identity and information assets

Domain Centric – User Centric IdM



User-Centric

Federation

User Provisioning

Maximum - Optimal User “control” and awareness “command” of Digital Identity

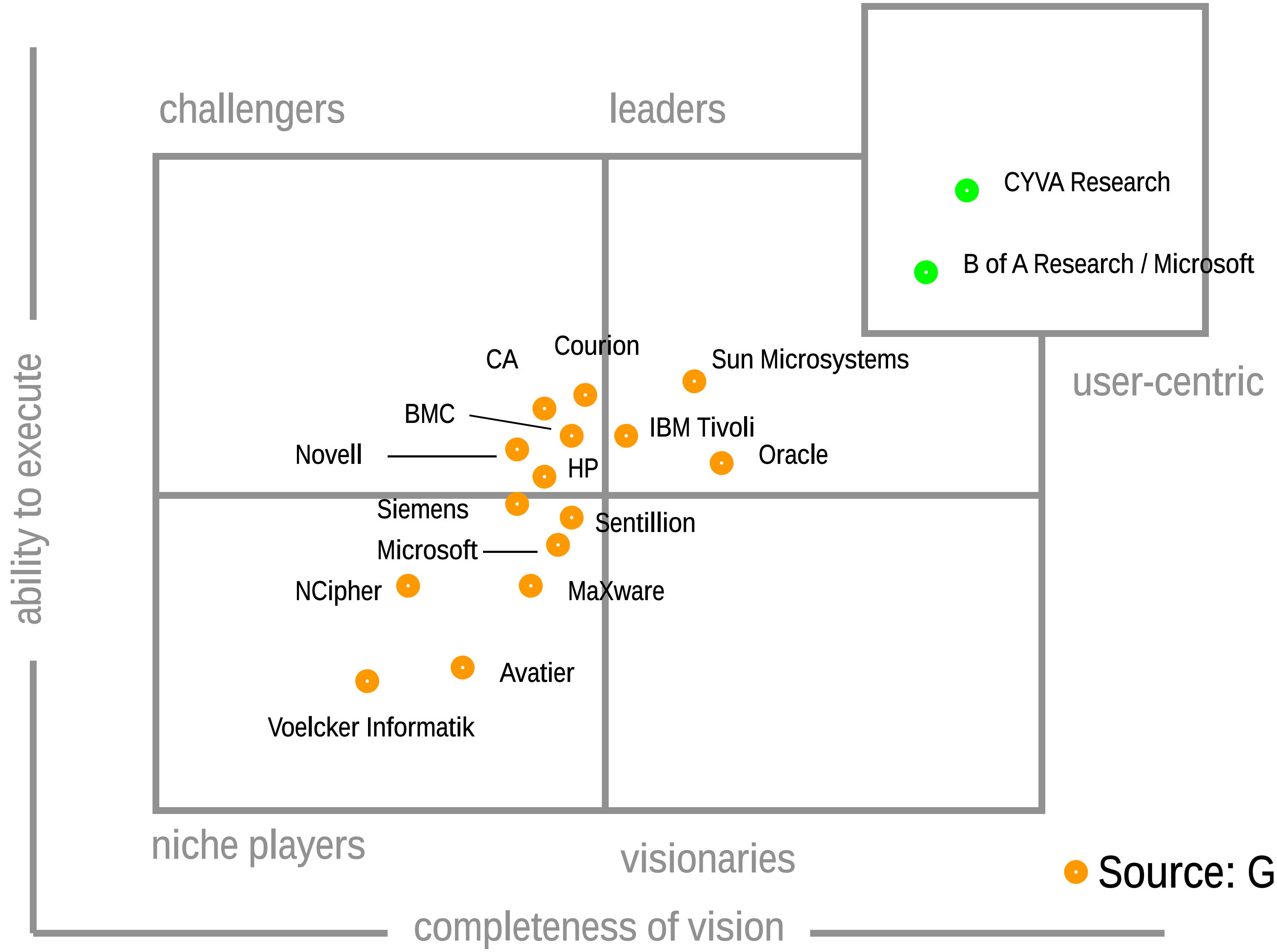
Single Sign-on

Meta Directories: Enterprise

LDAP Directories

Maximum Corporate “control”

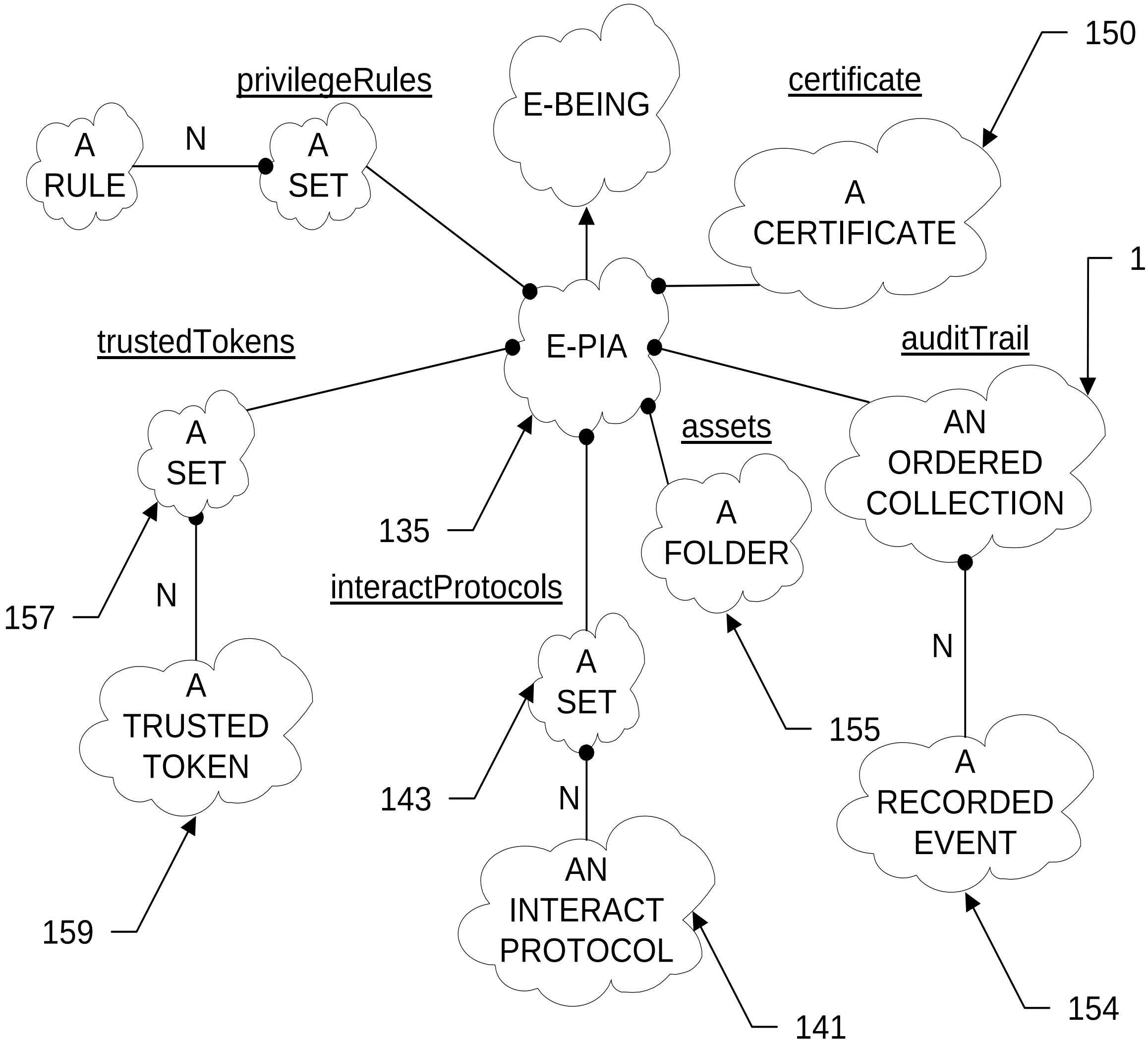
Next Magic Differentiator: User-Centricity



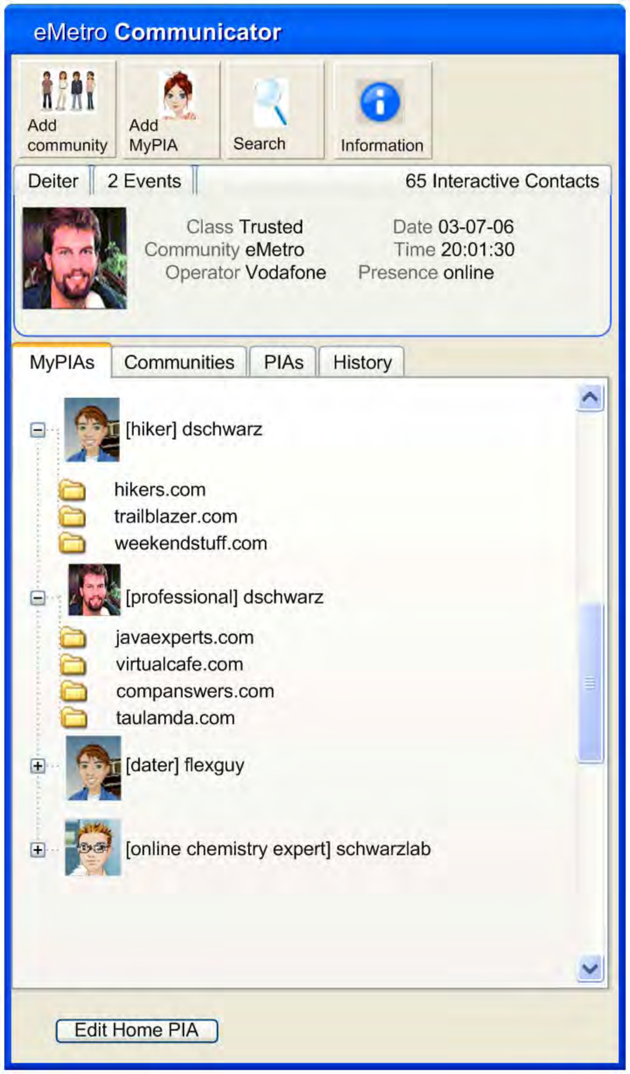
● Source: Gartner

Personal Information Agent ™

Self-determining Digital Persona



Personal Information Agent™



Deiter | 2 Events | 65 Interactive Contacts

Class Trusted
Community eMetro
Operator Vodafone

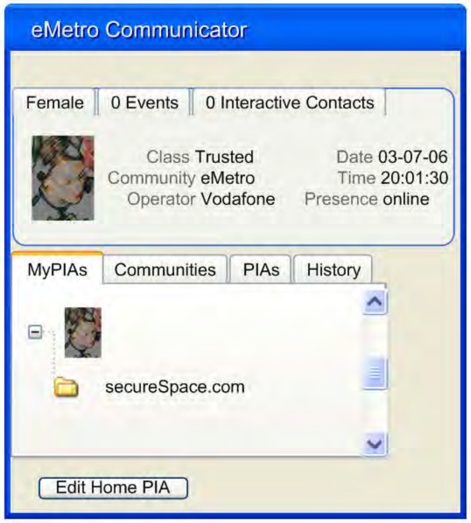
Date 03-07-06
Time 20:01:30
Presence online

[hiker] dschwarz
hikers.com
trailblazer.com
weekendstuff.com
[professional] dschwarz
javaexperts.com
virtualcafe.com
companswers.com
taulamda.com
[dater] flexguy
[online chemistry expert] schwarzlab

- Trusted Identity & Reputation
- Secure Personal Information (PI)
- Monitor and Manage PI
- Secure Messaging & Alerts

User-Controlled Identity

Anonymous



Class Trusted
Community eMetro
Operator Vodafone
Date 03-07-06
Time 20:01:30
Presence online

secureSpace.com

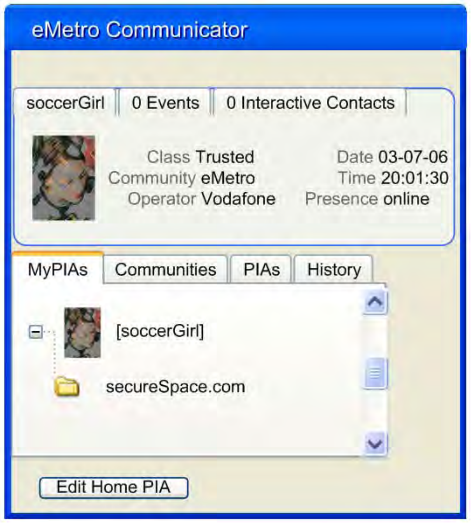
Trusted Anonymous Identity

Female

14

Traceability: None

Pseudonymous



Class Trusted
Community eMetro
Operator Vodafone
Date 03-07-06
Time 20:01:30
Presence online

[soccerGirl]

secureSpace.com

Trusted Pseudonymous Agent

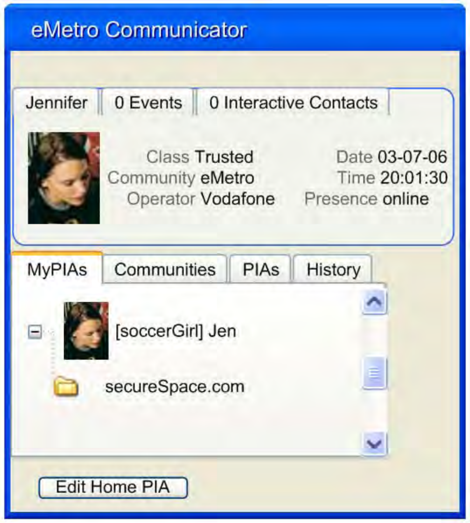
soccerGirl

Female

14

Traceability: P-nym

Veronymous



Class Trusted
Community eMetro
Operator Vodafone
Date 03-07-06
Time 20:01:30
Presence online

[soccerGirl] Jen

secureSpace.com

Trusted Veronymous Agent

Jennifer

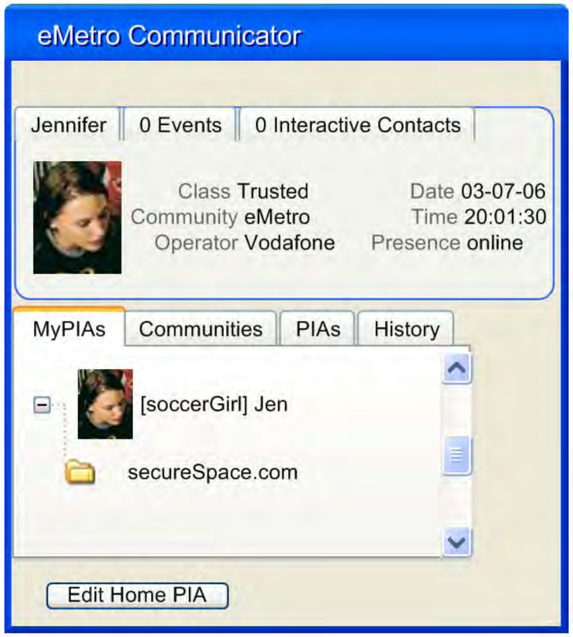
Female

14

Traceability: V-nym

Trusted Agent-based Marketing

- You want a piece of me…
  - My time
  - My attention
  - My data
- Talk to my agent… my Personal Information Agent (myPIA)
  - Negotiate and enforce rules for trusted (secure and verifiable) data use
  - User controlled identity: anywhere, anytime
    - User-controlled identity interactions and resolution: anonymous, pseudonymous, fully identifiable "veronymous"
  - New means to protect Mobile TV advertising experience "Dirty vs. Green" advertising



eMetro Communicator

Jennifer | 0 Events | 0 Interactive Contacts

Class Trusted
Community eMetro
Operator Vodafone

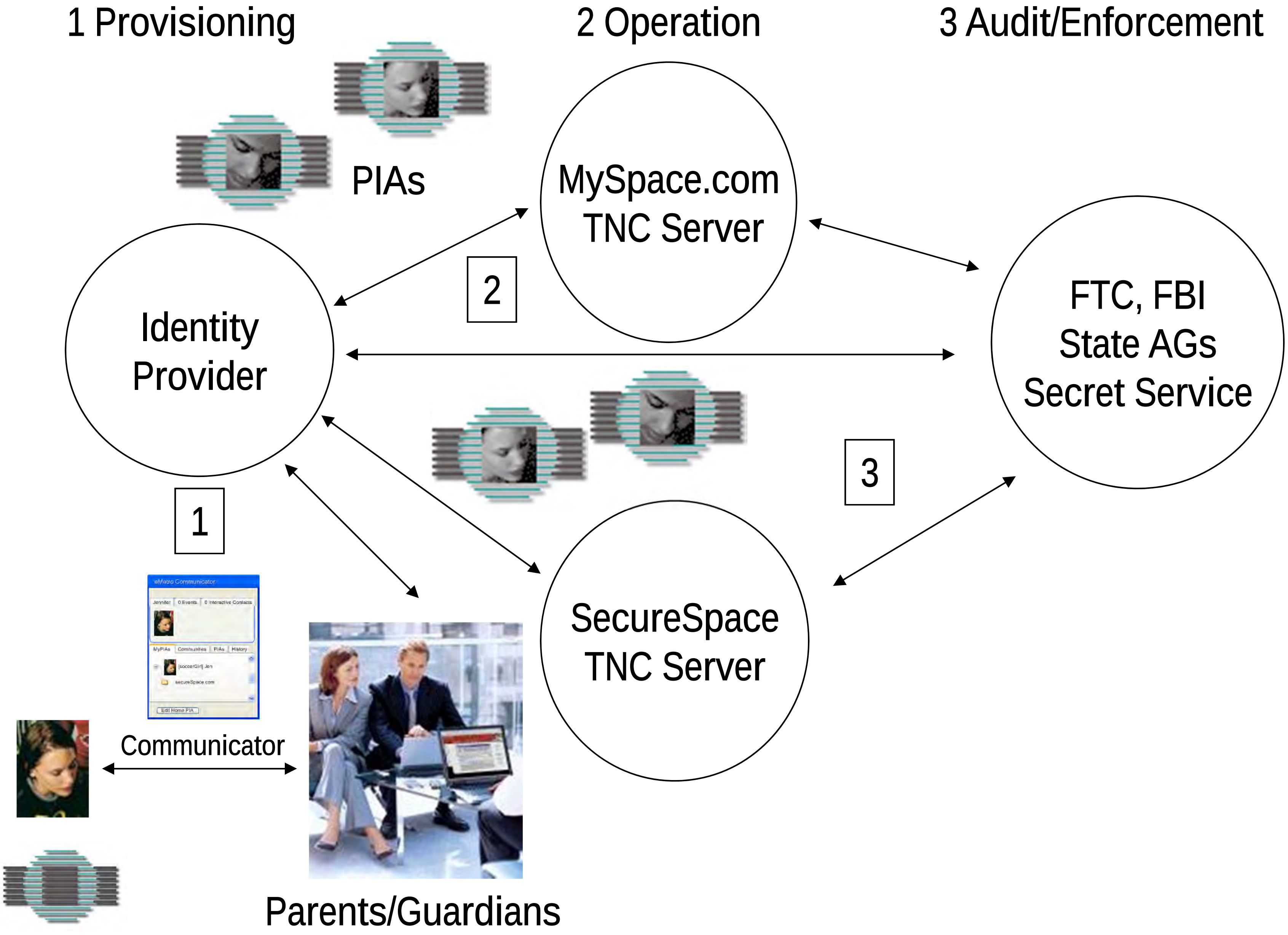
Date 03-07-06
Time 20:01:30
Presence online

MyPIAs | Communities | PIAs | History

[soccerGirl] Jen

secureSpace.com

Trusted Network Community Operation



1 Provisioning

2 Operation

3 Audit/Enforcement

PIAs

MySpace.com TNC Server

Identity Provider

FTC, FBI
State AGs
Secret Service

SecureSpace TNC Server

1

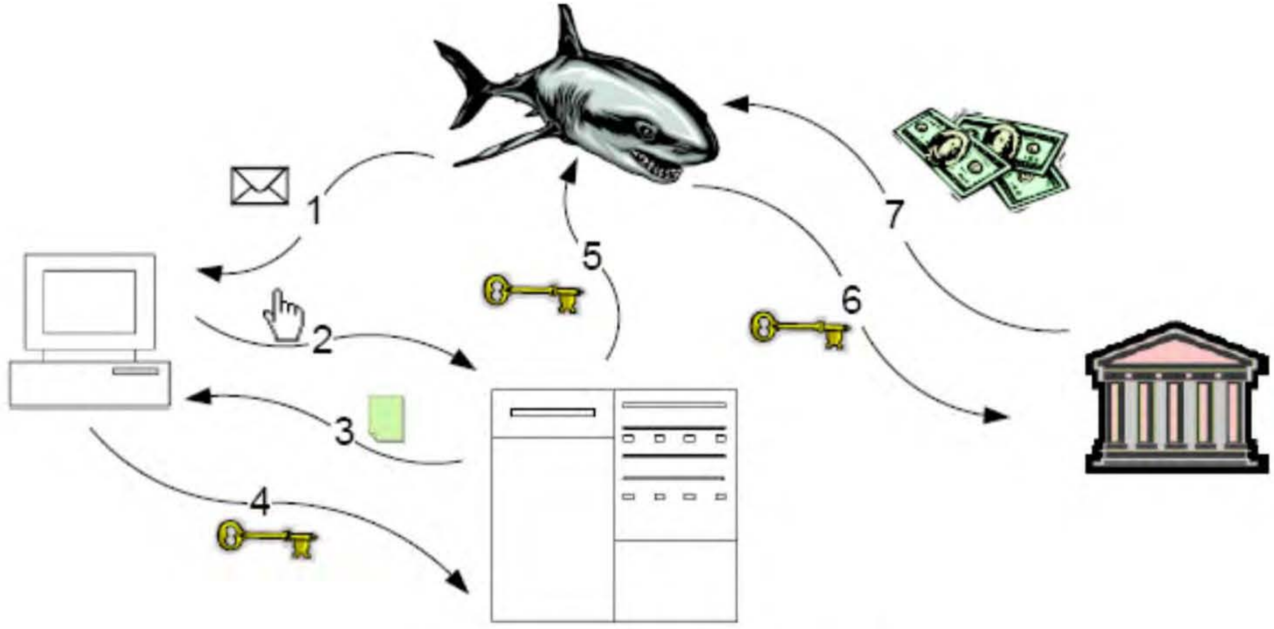
2

3

Communicator

Parents/Guardians

Present Phishing Vulnerability



Steps in a Phishing Attack

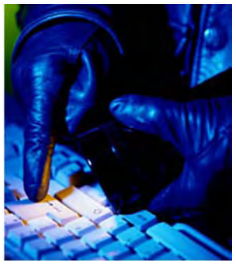
Making Stolen Data Useless & A Trap for Thieves

Fake currency

Stolen identity and data

Attempts to re-enter data to digital system for exploitation

Captures data by reading application or other sources



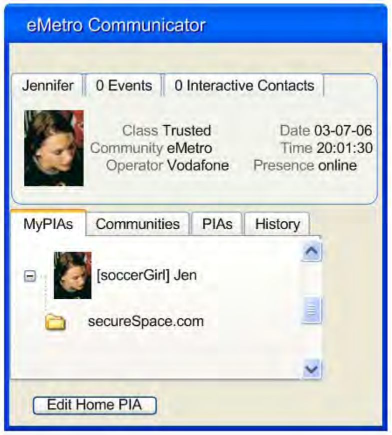
Applications recognize non-authentic data and compare to authentic Id, data and rules

Signal identity provider and consumer

Trusted feedback to processor and enforcement authorities

Authentic currency

Authentic identity, data and rules



eMetro Communicator

Jennifer | 0 Events | 0 Interactive Contacts

Class Trusted
Community eMetro
Operator Vodafone

Date 03-07-06
Time 20:01:30
Presence online

MyPIAs | Communities | PIAs | History

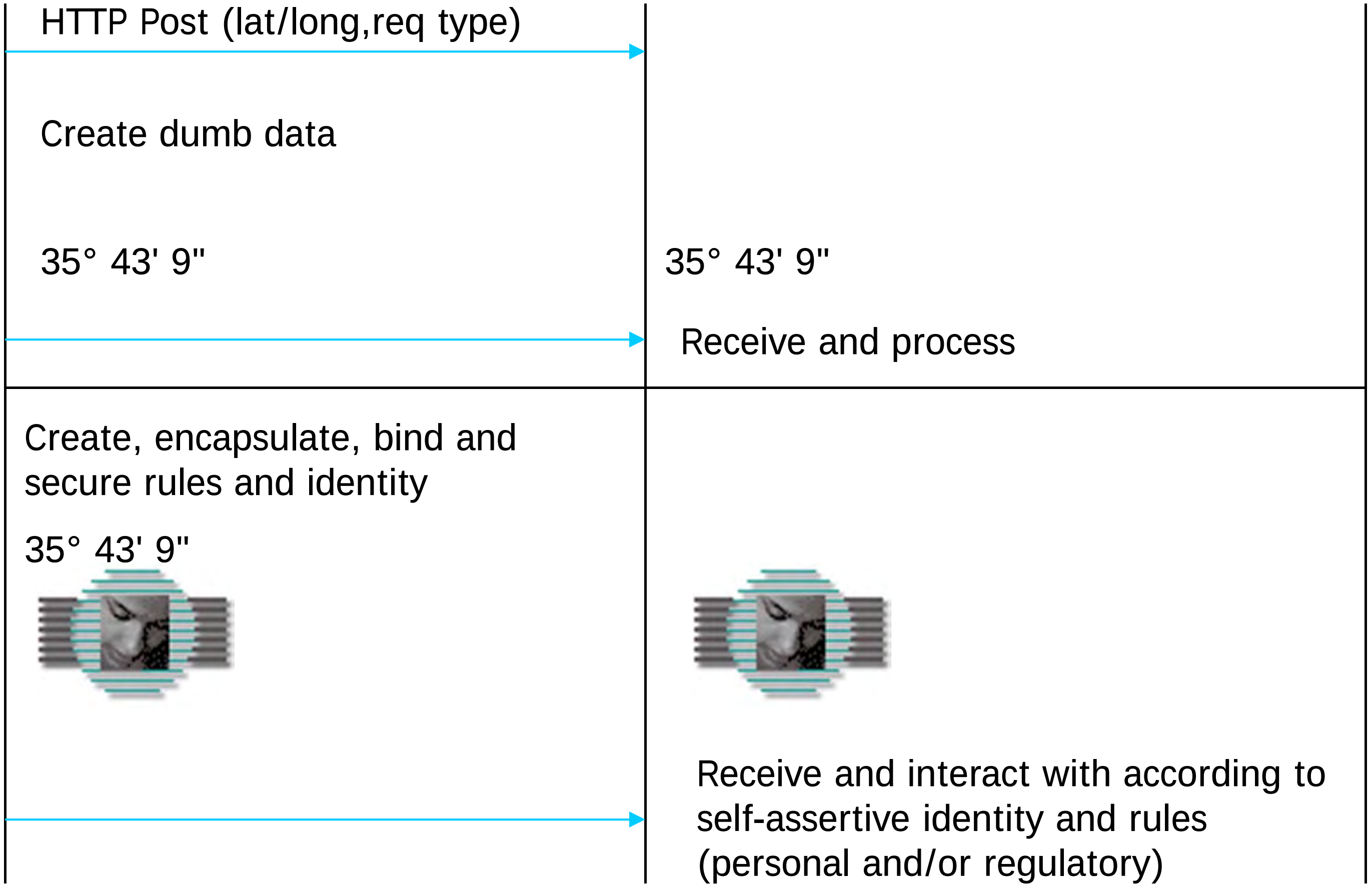
[soccerGirl] Jen

secureSpace.com

Edit Home PIA

Trusted feedback loop to customers and pre-set rules governing data (credit cards…)

Dumb Data vs. Intelligent Self-Protecting Agent



HTTP Post (lat/long,req type)

Create dumb data

35° 43' 9"

35° 43' 9"

Receive and process

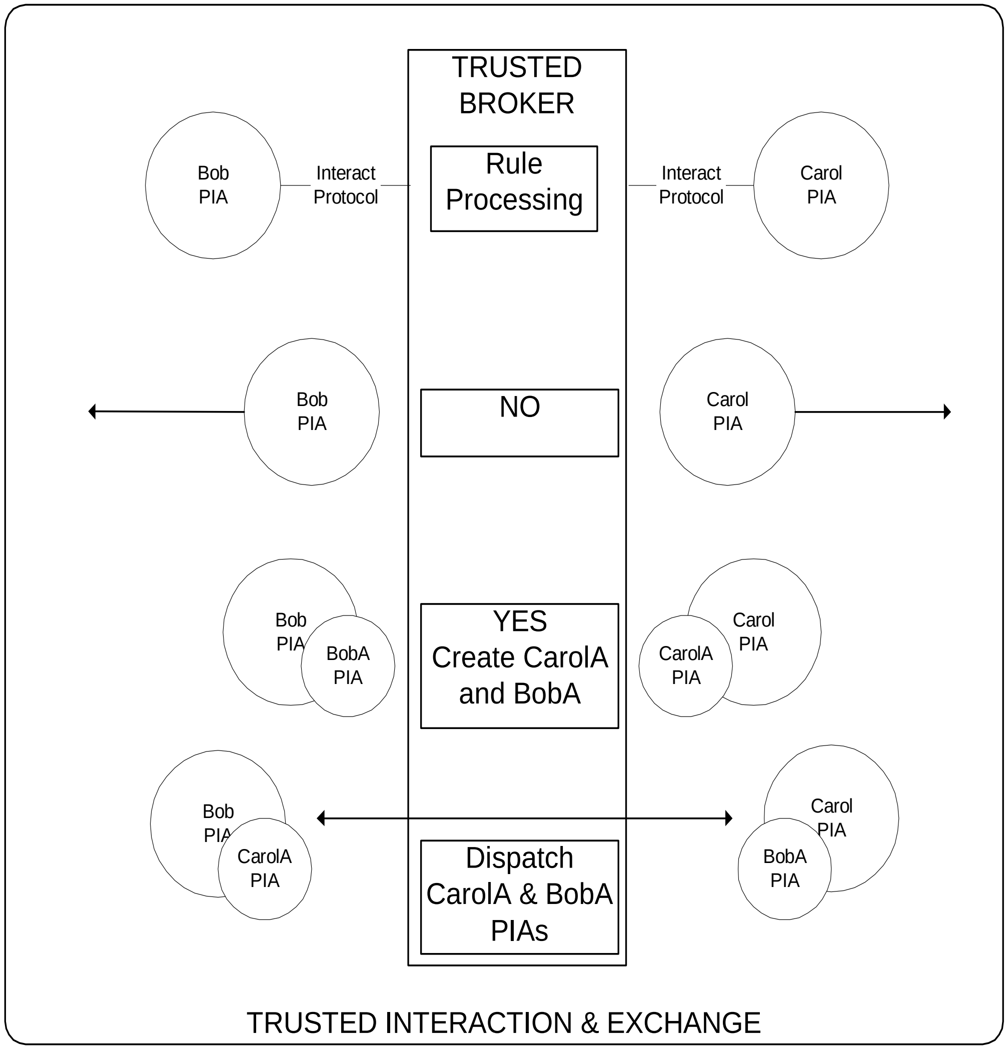
Create, encapsulate, bind and secure rules and identity

35° 43' 9"

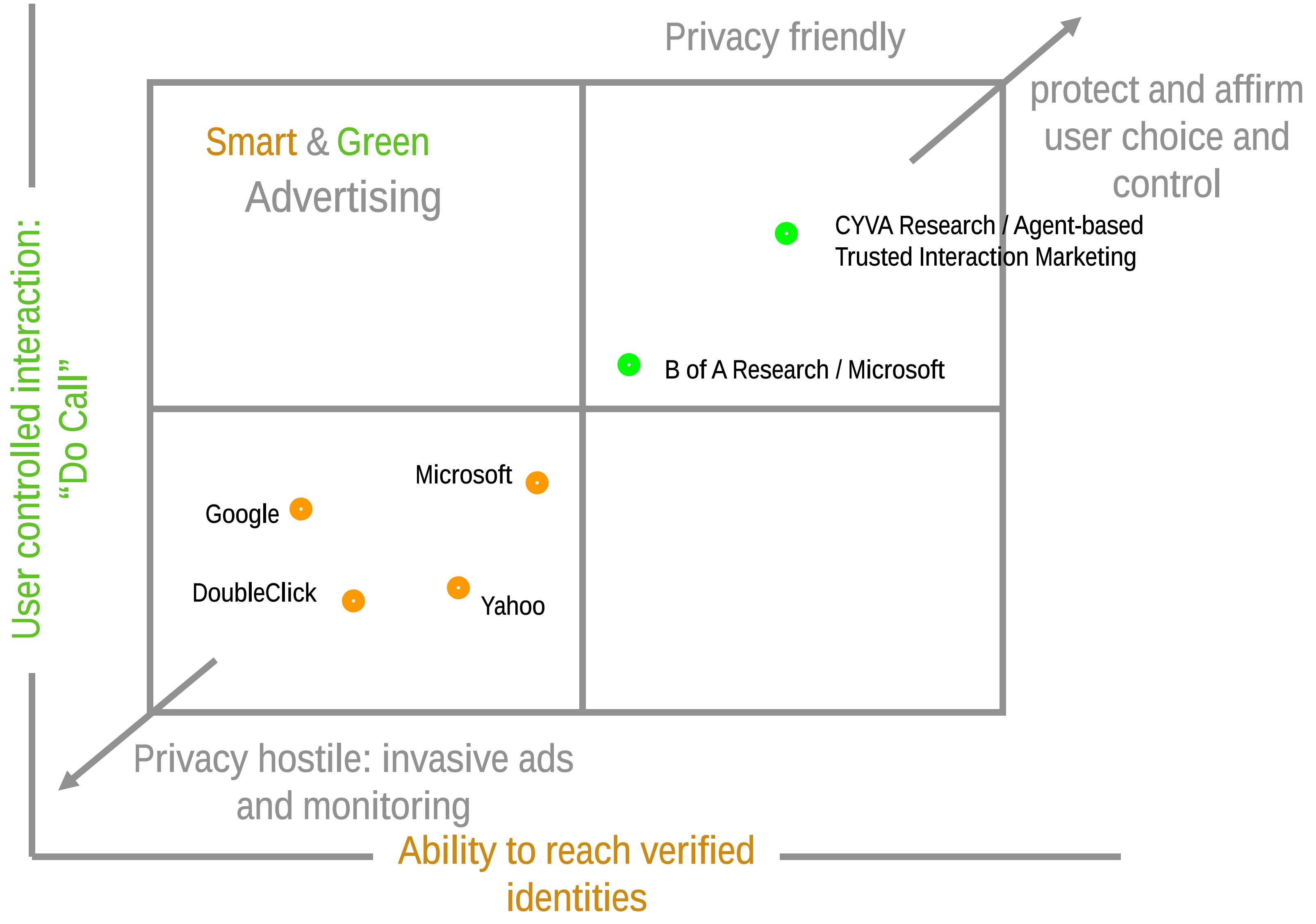
Receive and interact with according to self-assertive identity and rules (personal and/or regulatory)

Personal Information Agent ™

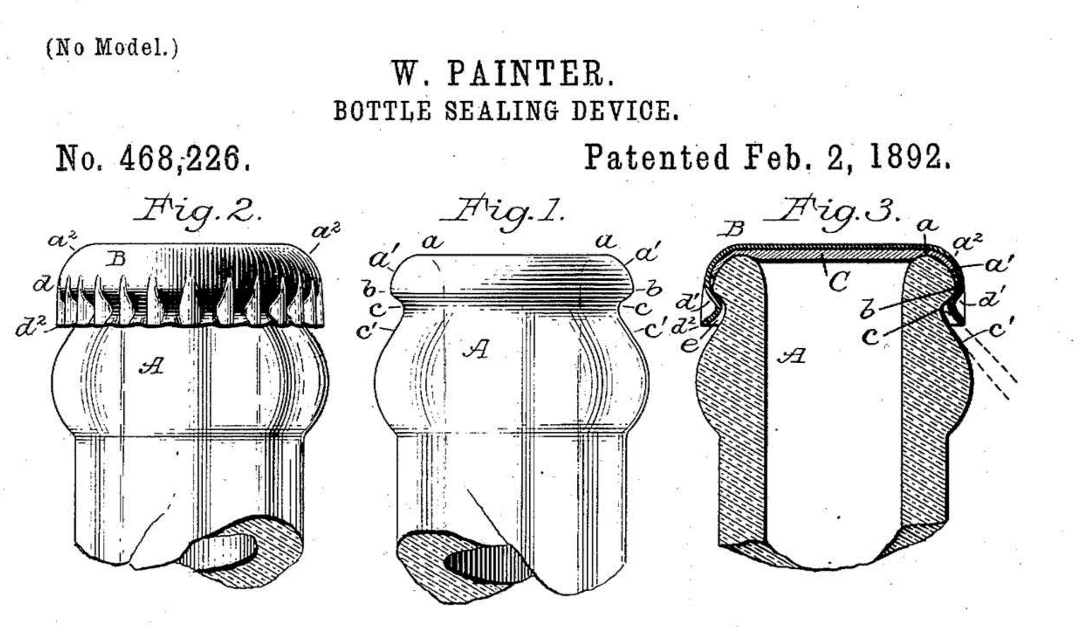
Trusted Interaction & Persistent Rules



Empowerment & Revenue Generation


Privacy friendly
protect and affirm user choice and control
Smart & Green Advertising
CYVA Research / Agent-based Trusted Interaction Marketing
B of A Research / Microsoft
Microsoft
Google
DoubleClick
Yahoo
Privacy hostile: invasive ads and monitoring
User controlled interaction: "Do Call"
Ability to reach verified identities

Recognize this Invention?



(No Model.)

W. PAINTER.

BOTTLE SEALING DEVICE.

No. 468,226. Patented Feb. 2, 1892.

Addressing & Advancing Privacy

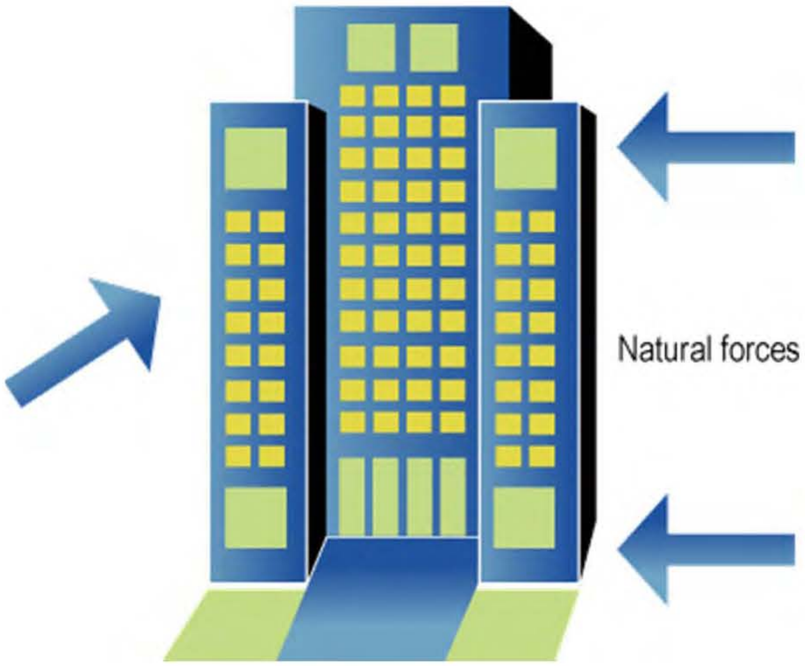
- Privacy today is alchemy. Advancing privacy as a discipline will require leveraging and adopting a hybrid set of know-how, tools, methods and paradigm.
  - Frameworks, models, and taxonomies represent a converging set of tools and engineering discipline that will advance the design and development of privacy assurance infrastructure.
  - Privacy officers, architects and engineers represent a nascent team of professionals that will collaboratively advance assurance infrastructure.
  - Essential to advancing privacy and developing solutions will be the adoption of practices, disciplines and accountability regimes borrowed from other professions and lessons learned.
  - Privacy defined and advanced as informational self-determination represents a paradigm shift that will significantly impact an evolving information culture and industry as we know it.

Privacy Architecture & Engineering

Agenda

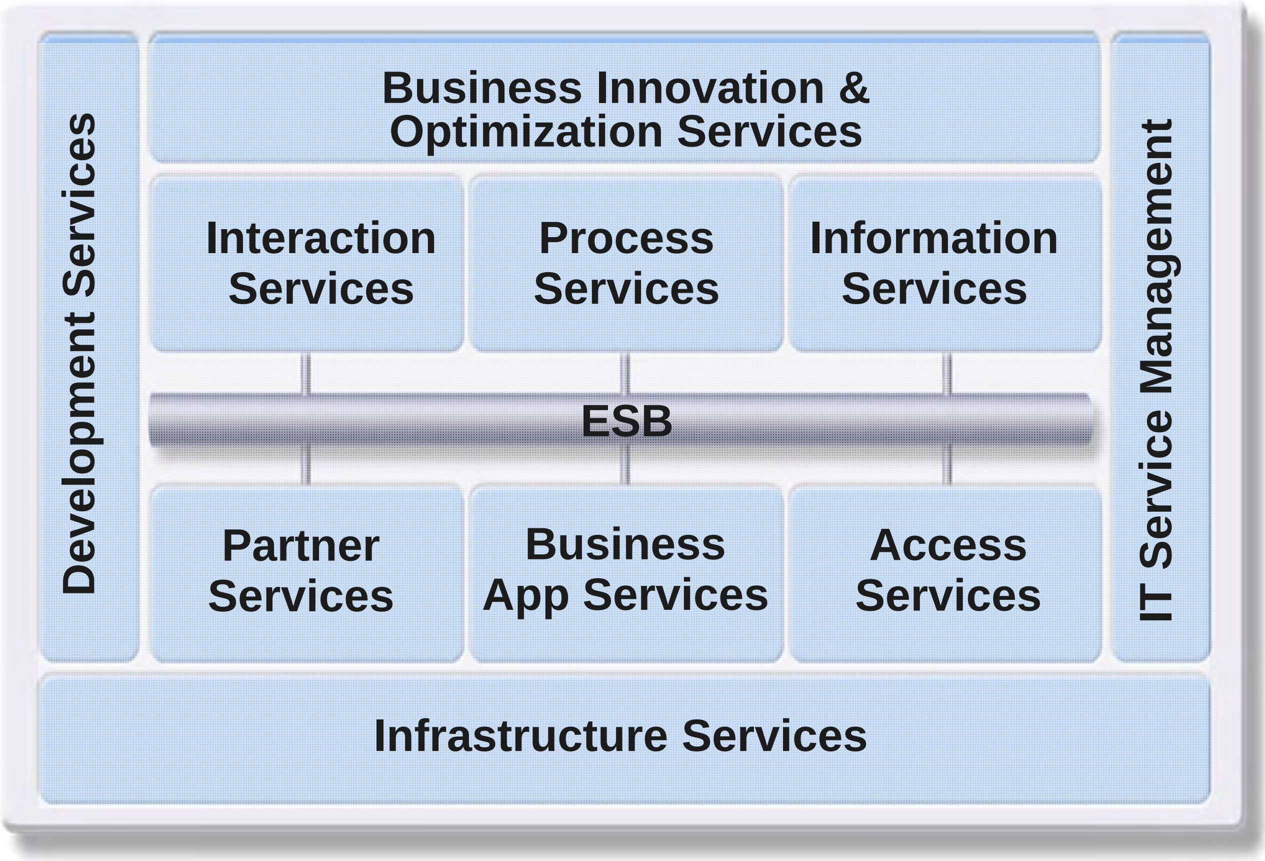
- Analysis: Privacy Essentials
  - Multifaceted Nature
  - Privacy Forces
  - Competition for Control
- Potential Data Protection Futures
  - Use & Misuse Cases
  - Privacy Taxonomy
  - *Frameworks & Architectures*
- Recommendations

Addressing Privacy & Security



Robust Capabilities Connected in an Open, Flexible Manner

IBM's SOA Reference Architecture



Modular product portfolio built on open standards

Functionally rich, adopted incrementally

Simple to develop, deploy and manage

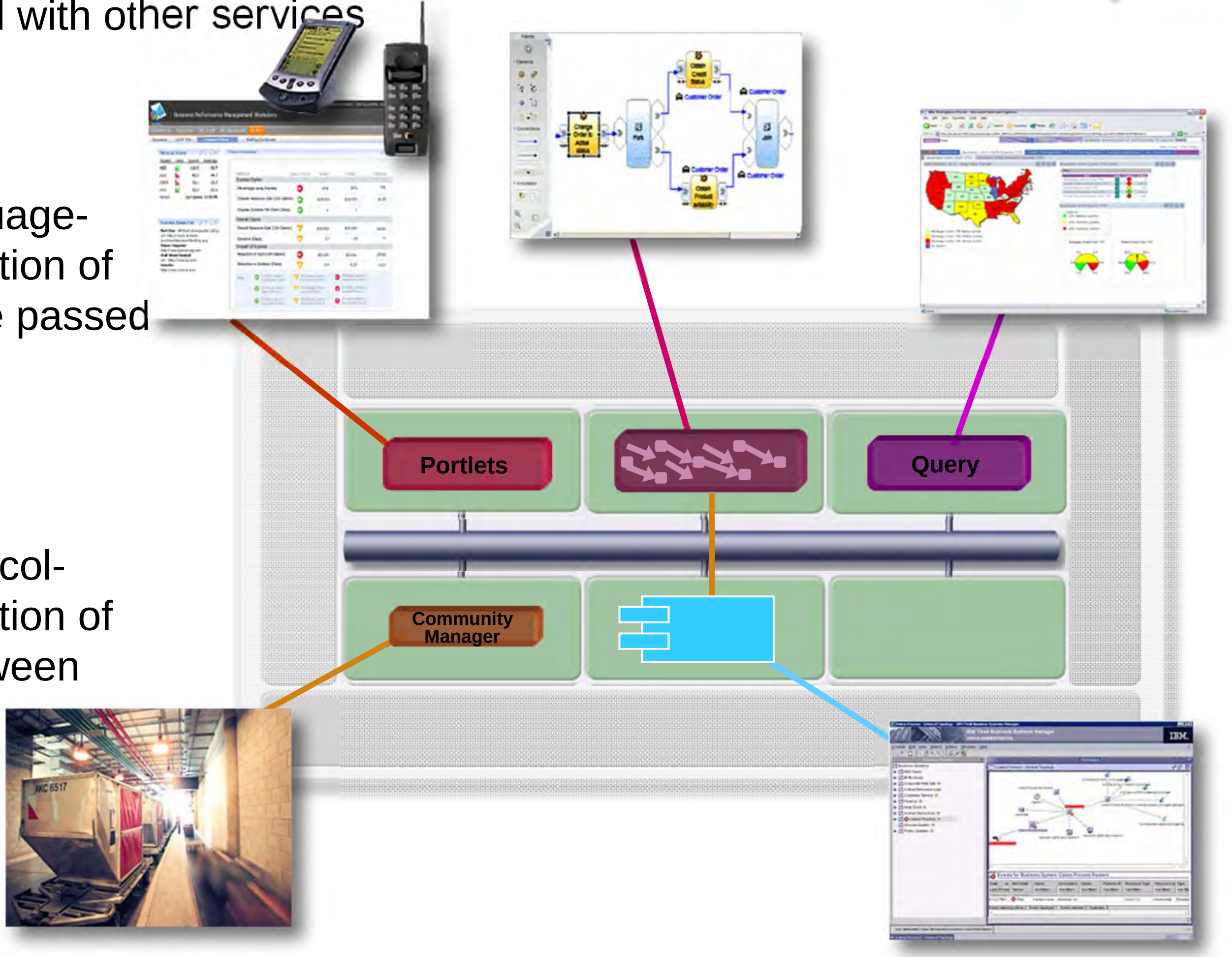
Integrated role-based tools for development & administration

…delivering the value of SOA, today

Source: IBM SHARE Orlando 2008 Conference, Session 5301

Core Elements of a Service-based Design

- Service Components
  - A technology- and language-independent representation of a service which can be composed with other services
- Service Data
  - A technology- and language-independent representation of a data entity that can be passed between services
- Service Bus
  - A technology- and protocol-independent representation of the interconnection between services



Source: IBM SHARE Orlando 2008 Conference, Session 5301

Frameworks & Architecture

Governance Frameworks & Compliance-oriented Architecture

- ISTPA Privacy Framework
  - Translating law (Latin) into operational infrastructure (Greek)
  - Leverage SOA
  - Services reference model
- Compliance architectural patterns
  - IBM Risk & Compliance Framework
  - Computer Associates' Compliance Management Framework
  - RedMonk's Compliance Oriented Architecture (COA)
  - RSA Security, others
- Emerging but disparate compliance framework efforts
  - Need for standards approach
  - Repository of compliance architectural patterns addressing diverse compliance requirements
  - Currently vendor solution focus with mapping to compliance requirements

Frameworks & Architecture

Principle	OECD	EU Directive	Safe Harbor	PIPEDA	AICPA/CICA	ISTPA
Ensure accuracy of collected personal information	Data quality	Data quality	Data integrity	Accuracy	Quality	Validation
Disclose to individuals reasons why collection of each item of information is necessary	Purpose specification	Information given to the data subject (Section IV)	Notice	Identifying purposes	Notice	Interaction
Protect personal information from unauthorized access	Security safeguards	Confidentiality and security of processing (Section VIII)	Security	Safeguards	Security	Control

Frameworks & Architecture

Translating Law to Operational Infrastructure

- Individual Access

  “enable individual to challenge accuracy and completeness of personal information (PI) in your control”

Privacy Framework Services									
Access	Agent	Audit	Certification	Control	Enforcement	Interaction	Negotiation	Usage	Validation
X	X			X		X			X

Frameworks & Architecture

ISO/OSI Model		
Layer	Function	Protocol
Application	Specialized network functions such as file transfer, virtual terminal, electronic mail, and file servers.	DNS, TFTP, BOOTP, SNMP, RLOGIN, FTP, SMTP, MIME, NFS, FINGER
Presentation	Data formatting and character code conversion and data encryption.	
Session	Negotiation and establishment of a connection with another node.	
Transport	Provision for reliable end-to-end delivery of data.	TCP, UDP
Network	Routing of packets of information across multiple network.	IP, ARP, RARP, ICMP, RIP, OSPF, BGP, IGMP
Data-link	Transfer of addressable units of information, frames, and error checking.	SLIP, CSLIP, PPP, MTU
Physical	Transmission of binary data over a communications network.	ISO 2110, IEEE 802, IEEE 802.2

Frameworks & Architecture

ISTPA Privacy Framework as Reference Model		
Service/Capability	Function	Organizations/Protocols/Mechanisms
Certification	credentials, trusted processes	BBBOnline, BetterWeb, E-Safe, Global Trust Alliance, Guardian eCommerce Security, Net-Ethix, Privacy License, Privacy Secure, Inc., PrivacyBot.com, SecureBiz, TRUSTe, WebTrust
Validation	checks accuracy of personal information	Audit Check Services, Certificate Authorities, Credit Check Services,
Negotiation	of agreements, rules, privileges	APPEL, P3P, EPAL, License Script, FDRM, ODRL, XrML
Usage	data use, aggregation, anonymization	Trusted Computing Group, Trusted Platforms, Smartcards, Secure Tokens
Security Foundation		
Mechanisms		AES, MD5, Authentication, Non-Repudiation, Access Control, Integrity, Confidentiality, Availability, PKI
Legal Context		
Legal, Regulatory, Policy		EU Data Protection Directive, HIPAA, GLBA, COPPA, Privacy Act

Source: ISTPA

Privacy Language & Taxonomy

Privacy Taxonomy

- Privacy taxonomy dimensions permit the expression of rules of the form:

  Subject to <conditions> and <security> requirements,
  allow <action> for <purpose>,
  where data are <category> about <identity>,
  from <source> to <recipients>,
  with <obligations> and <retention requirements>.

Source: Government of Alberta

Privacy Taxonomy

ID Taxonomy

- An identity taxonomy will aid the design of privacy features for future products and services
  - “Trusted anonymous to pseudonymous to verynymous identity”*
  - “Nymity - the continuum from anonymity through pseudonymity to verynimity. Anonymous location services pose less of a concern to privacy. Many location services need not be verynymous, i.e. how do I get to the nearest 4-star hotel or 'Send a police car‘”*

Source: Liberty Alliance

Privacy Taxonomy

ID Taxonomy

- An identity taxonomy will aid the design of privacy features for future products and services
  - The Trusted Computing Group (TCG) has designed-in the privacy principle of choice. The platform owner has the choice to opt-in or opt-out of the use of an Attestation Identity Key (AIK). This feature of the Trusted Platform Module (TPM) provides owners greater flexibility, opt-in, opt-out, multiple AIKs, providing choice-control of which AIK to use for a given transaction.
  - Direct Anonymous Attestation (DAA) is a means for the individual platform owner to create their own platform attestation key without communicating explicitly the identity of their platform. DAA enables attesting to being on a trusted platform without revealing identity.

Source: Trusted Computing Group

Privacy Architecture & Engineering

Agenda

- Analysis: Privacy Essentials
  - Multifaceted Nature
  - Privacy Forces
  - Competition for Control
- Potential Data Protection Futures
  - Frameworks & Architectures
  - Use & Misuse Cases
  - Privacy Taxonomy
  - *Paradigm Shift: Architects, Engineers & Social Responsibility*
- Recommendations

Architects, Engineers & Social Responsibility

Practices, disciplines and accountability regimes

- The design and construction of buildings, automobiles, and the protection of our ecological environment have each benefited from the adoption of practices, disciplines and accountability regimes.
- Certification implies an assurance that an individual possesses a specific knowledge or skill level pertaining to an occupation.
- Under licensure laws, it is illegal for a person to practice a profession without first meeting state standards.

Architects, Engineers & Social Responsibility

Practices, disciplines and accountability regimes

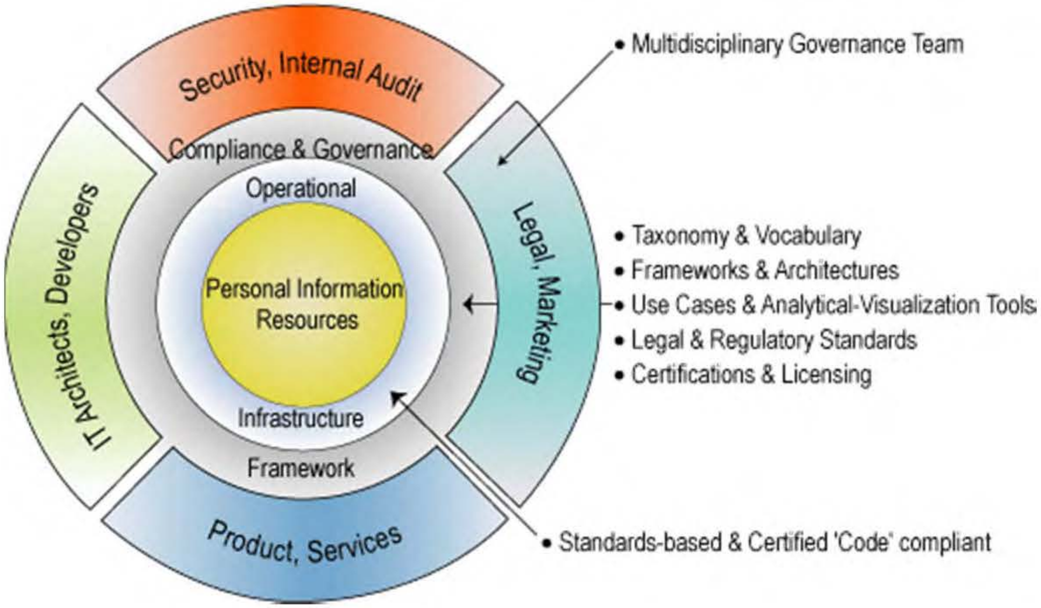
- Architects, structural and mechanical engineers are certified and licensed professionals.
- Engineering disasters and catastrophes drove the adoption and development of certification and licensing.
- The emergence of ‘green’ building architecture and design in response to energy and environmental concerns is indicative of forces that continue to influence a licensed profession.
- Within the privacy domain there is a well documented litany of harm, abuse and growing fear of a surveillance society.
- 1 Million dead and the publication of *Unsafe At Any Speed; The Designed-In Dangers Of The American Automobile* drove federal mandates for automobile safety standards.

Privacy Architecture & Engineering

Agenda

- Analysis: Privacy Essentials
  - Multifaceted Nature
  - Privacy Forces
  - Competition for Control
- Addressing Privacy
  - Frameworks & Architectures
  - Use & Misuse Cases
  - Privacy Taxonomy
  - Paradigm Shift: Architects, Engineers & Social Responsibility
- Recommendations & Questions

Recommendations



- Multidisciplinary Governance Team

- Taxonomy & Vocabulary
- Frameworks & Architectures
- Use Cases & Analytical-Visualization Tools
- Legal & Regulatory Standards
- Certifications & Licensing

- Standards-based & Certified 'Code' compliant

Recommendations

Privacy Governance

- To understand, address and competitively adapt to the diverse array of privacy forces a standing team of interdisciplinary practitioners needs to be empowered and charged with an enterprise wide mission.
  - Legal
  - Marketing
  - Product and Service
  - Security & Internal Audit
  - IT Architects & Developers

Recommendations

Privacy Governance

- Not only should a centralized (policy administration) and interdisciplinary team (distributed) address privacy but such a team should examine closely the compliance spectrum (e.g., Sarbanes- Oxley, Basel II, US Patriot Act) and devise a compliance framework and plan to leverage compliance infrastructure investments across multiple regulatory requirements.
- Such a team can provide a strategic assessment of how not only to leverage and lower compliance cost but provide insight into entering and creating new disruptive capabilities.

Recommendations

Privacy Compliance & Governance

- CPOs and CGOs
- Compliance generalist and multi-disciplinary compliance professional teams
- Constructing buildings – Constructing infrastructure
  - Certified-licensed architects, structural, and mechanical engineers and building contractors and inspectors
  - Certified-licensed IT architects, developers, security, audit and legal
  - Ongoing questions of regulatory or market approaches to privacy

Recommendations

Privacy Governance & Compliance Architecture

- ***Integrated and intelligent buildings are becoming the norm:*** Today's architects must consider green and sustainable design, security, audio/video automation, convenience devices, advanced HVAC systems and data-driven building information modeling.*

Source: California Architects Board
Summer 2004 Newsletter

Recommendations

Privacy Governance & Compliance Architecture

- Integrated and intelligent infrastructure is becoming a reality and privacy is much like the ‘green’ ecological requirements impacting building design today. Socially responsible enterprise infrastructure that empowers privacy and security as dual and attainable objectives will not only survive but prove a sustainable business.

Source: California Architects Board
Summer 2004 Newsletter

Recommendations

Privacy Pragmatism

- Architect and engineer a flexible, adaptive, compliance infrastructure: privacy and a litany of disjointed regulatory requirements will continue to churn, plan on it.
  - Internally and externally conflicted organizational perspectives and agenda will continue for some time.
  - Domestic and international regulatory ‘legal’ frameworks will seek a harmonized view but the regulated will struggle at the detailed how to implement level. “I understand why but tell me how to comply.”
  - Managing the regulatory compliance details will continue to be a non-trivial challenge but privacy management tools: frameworks, models and taxonomies and analytic tools will help alleviate the disruption of continued regulatory changes and complexity.
  - Vendors see the need and compliance is a driving force behind new offerings but again, the details of how they actually support compliance is to be determined, more later.

Recommendations

Privacy Long Term

- Certification and Licensure
  - Systems architects
  - Security architects
  - Software Developers
  - Audit and Compliance professionals

Recommendations

Privacy Long Term

- Growing Awareness and Sensitivity
  - Pivotal awareness
  - Translates to Political Action
  - Everyone becoming an advocate
- Privacy standards
  - Continued international clash and churn of competing interests
  - ISO/IEC JTC 1 Privacy Technology Study Group recommendations
  - ISTPA/PETTEP Joint Effort to engage Data Protection Authorities

Recommendations

Privacy Long Term

- Risk Management, Compliance and Governance Frameworks
  - ISTPA Privacy Framework
  - Compliance-oriented Architecture (RedMonk)
  - Risk and Compliance Framework (IBM)
  - Compliance Management Framework (CA)
- Visualization and analytic tools
  - Policy languages and tools
  - Human and machine readable policy
  - Policy instantiation, actualization, monitoring
- Addressing and managing spaghetti law – spaghetti code syndrome
  - Tangled and piecemeal array of laws (GLBA, HIPAA, Sarbanes-Oxley,…)
  - Integrated and intelligent compliance infrastructure

Copyright Notice