



Identity in Context: Assessing Options for Maintaining Social Order in Online Spaces

Mike Neuenschwander
VP and Research Director
Burton Group
miken@burtongroup.com
www.burtongroup.com

Tuesday – April 4th, 2006



Identity in Context

2

Thesis

- “Freedom in a commons brings ruin to all”—G. Hardin
 - Shared information, like shared space, is a breeding ground for social dilemmas
 - How does society maintain order in an online environment?
- Classical social model: administrative intervention
 - A governing body guards the resource
 - Identification becomes the organizing construct for management
 - A wide variety of technologies have emerged to support this model
- But there’s always a greater context: a “meta-commons”
 - What’s the impact of millions of sites issuing billions of IDs?
 - Should there be an uber-ID? Linked IDs?
 - Should IDs be harder to fake? Harder to get?



Identity in Context

3

Thesis (cont'd)

- But what role do IDs play in maintaining social order?
 - (a profound question, on which I'll harangue and not attempt to bulletize a response to)
 - (This space intentionally left blank for your notes)
- Changing the role of the resource facilitator
 - Create conditions that promote community cohesion, which in turn creates resilience of the resource
- Placing the nail
 - Identification is really just a thing on which to hang reputation and at which to direct reciprocity



Agenda

- The social context
- A look at contemporary control systems
- What are other governments doing?
- Revisiting the role of identity
- Recommendations



Agenda

- *The social context*
- A look at contemporary control systems
- What are other governments doing?
- Revisiting the role of identity
- Recommendations



The Social Context

Pardon the indulgences

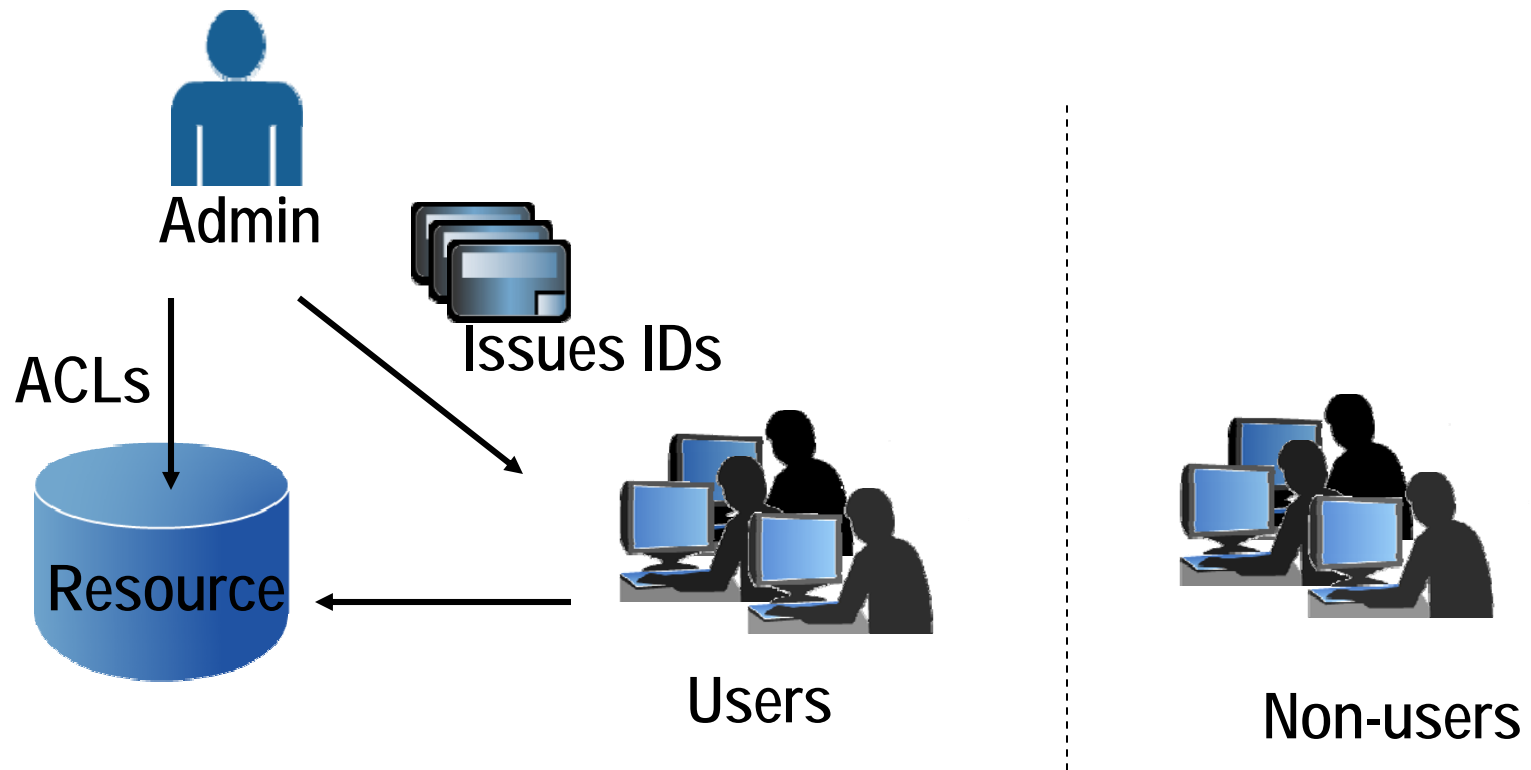
- This section is academic, for sure
- But hopefully for good cause
 - The issues we face with identity are largely social, not technical
 - Require some familiarity with socio-scientific jargon
- Disclaimer
 - I don't have a degree in social science
 - (although I could probably buy a SAML token that assures you I am)
 - This is an attempt to foster a discussion that introduces social theory into considerations around identity



The Social Context

Identity management today: the fully facilitated model

- Exclusion through identification





The Social Context

8

The rationality of facilitated domains

- The model is familiar and seems reasonable
- From an individual/admin perspective it's the right model
- But from a collective perspective, it's suboptimal
 - For the administrator
 - Has to manage the artifacts, set up access controls, monitor the environment—can become complex at scale
 - The admin must also be monitored and audited
 - For the individual
 - Identification overload
 - Risks exposure of identity information
 - For the organization
 - A good ID invites derivative use; but the organization doesn't want to assume burden of proof or responsibility outside the original context



The Social Context

Defining the variables: social concepts relevant to technology

- A social dilemma is
 - “the study of the tension between individual and collective rationality. In a social dilemma, individually reasonable behavior leads to a situation in which everyone is worse off” —[Peter Kollock](#)
 - aka collaborative / collective action problem
- Common pool resources: flashpoint for social dilemmas
 - A shared resource, marked by
 - Difficult and costly *exclusion*: can't easily put a fence around it
 - *Subtractability* (a rival good): use of the resource depletes it
- Externalities: the remainder of the social equation
 - Positive: returns value into the pool
 - Negative: a cost not borne by the use of the resource



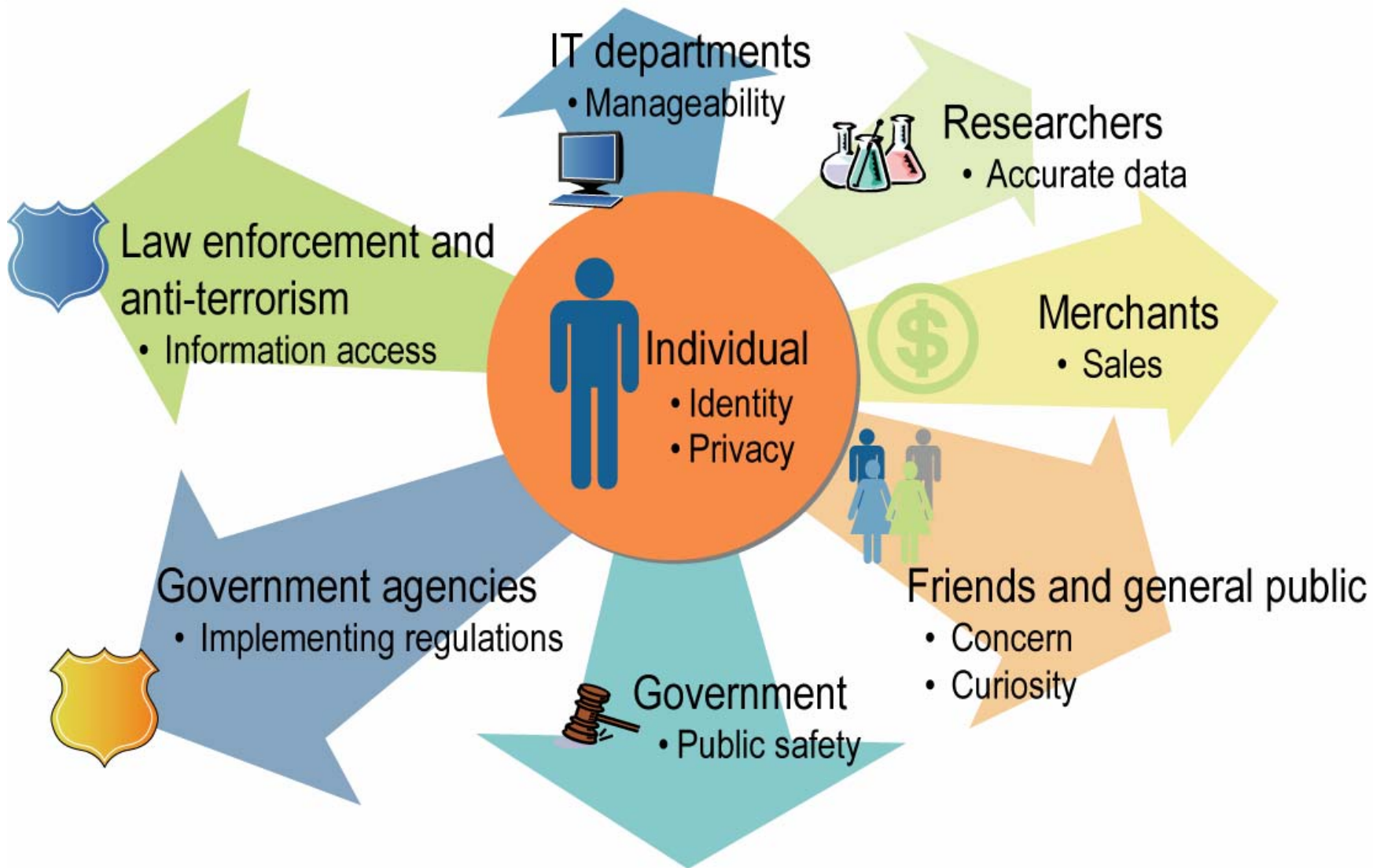
Identity as a social dilemma

- What qualifies identity as a social dilemma?
 - Identity is often used as a structural solution to social dilemmas
 - Identity information is itself a common pool resource (CPR)
 - Requires coordination among actors, but with few motivating drivers
- Identity as a structural solution
 - How to preserve a digital commons? Management and regulation of the resource (by issuing licenses, IDs, etc. and enforcing rules)
 - Creates negative externalities
- Identity as a CPR
 - Costly exclusion: keeping shared identity information private is extremely difficult
 - Subtractability: the more an attribute is used, the more public it becomes, the less valuable it is for proofing

The Social Context



Contention over a common pool resource





The Social Context

12

Examples and externalities of identity

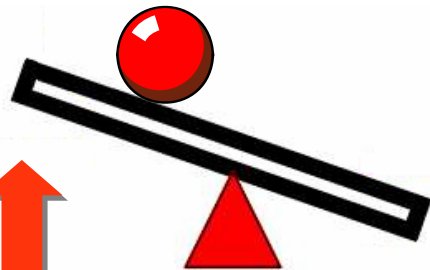
- Internet transactions
 - Require credit card, mailing address, home number, etc.
 - But what happens when a Google search can provide all that information about an individual?
- SSN's in the United States
 - Overuse of the SSN created all kinds of dependencies while making individual's SSNs public knowledge
- Personal costs
 - Identity theft, slander, persecution, prejudice, privacy invasion can result from identification linkage and identity information leakage
- Government intervention
 - Privacy legislation, data protection regulation, fair practices guidelines

The Social Context

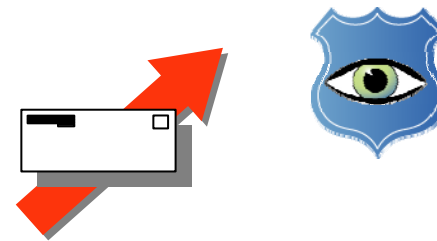


The problem with normal: the success catastrophe

Drawing the attention of criminals



Requiring government oversight



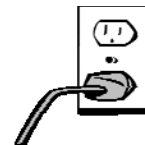
Making people angry



Security at the cost of reducing privacy and efficiency



Increases value of infrastructure



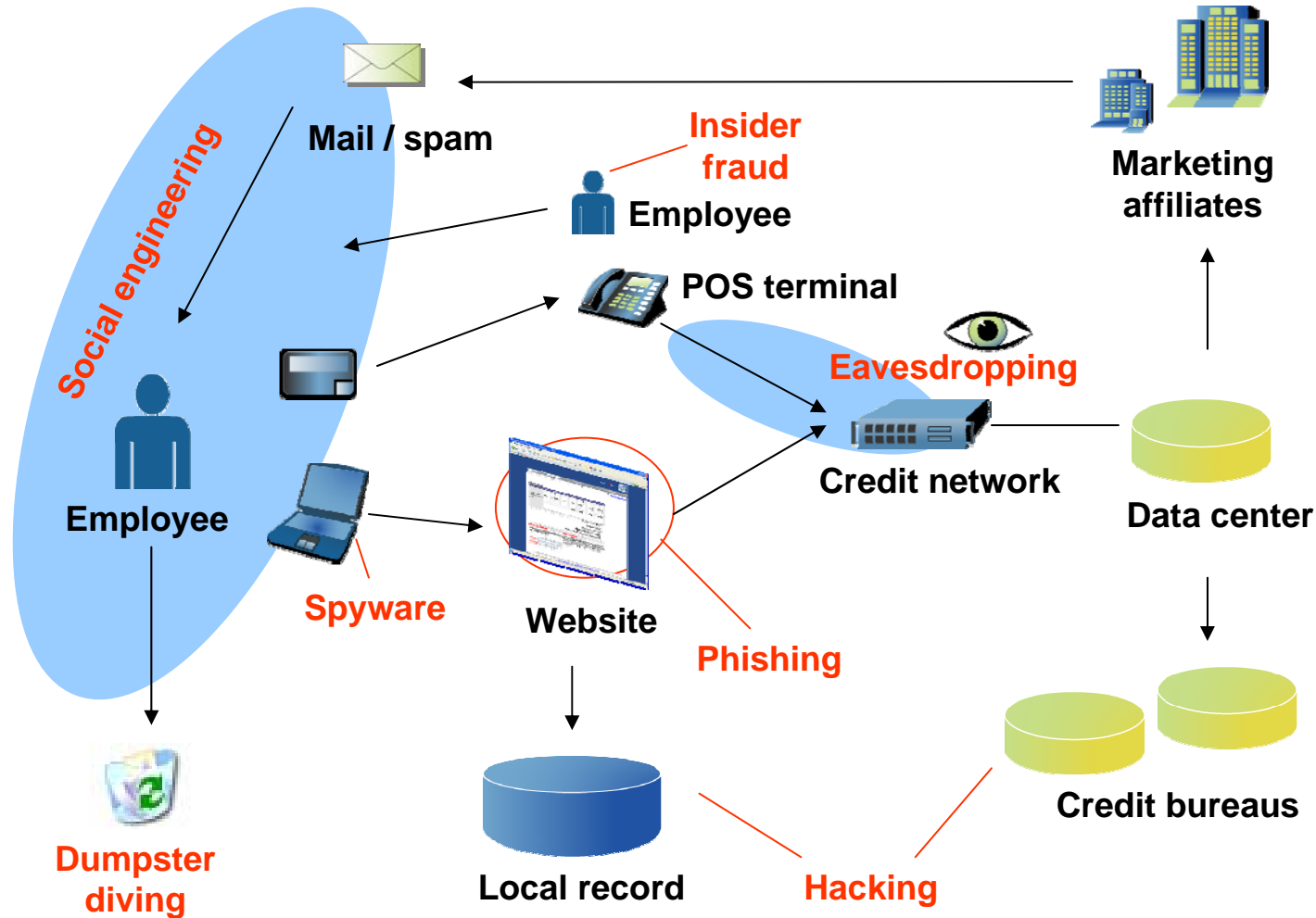
Greater connectivity for business



The Social Context



Architecture and its evil twin brother, the attack vector





The identity dilemma

- Administrative rationality vs. collective rationality
 - Generating IDs is rational behavior for individual resource owners
 - But it results in suboptimal outcomes at the extra-domain level
 - Not suggesting sharing identity information isn't worth the effort
 - But we have to consider the consequences
- How should resource owners/facilitators act?
 - A collaborative action problem: a solution only works if enough resource owners agree to behave in a coordinated fashion
- We'll return to these issues in a moment...



Agenda

- The social context
- *A look at contemporary control systems*
- What are other governments doing?
- Revisiting the role of identity
- Recommendations



Burton's categorical definition of IdM

Identity management is

the set of **business processes**,

and a **supporting infrastructure**,

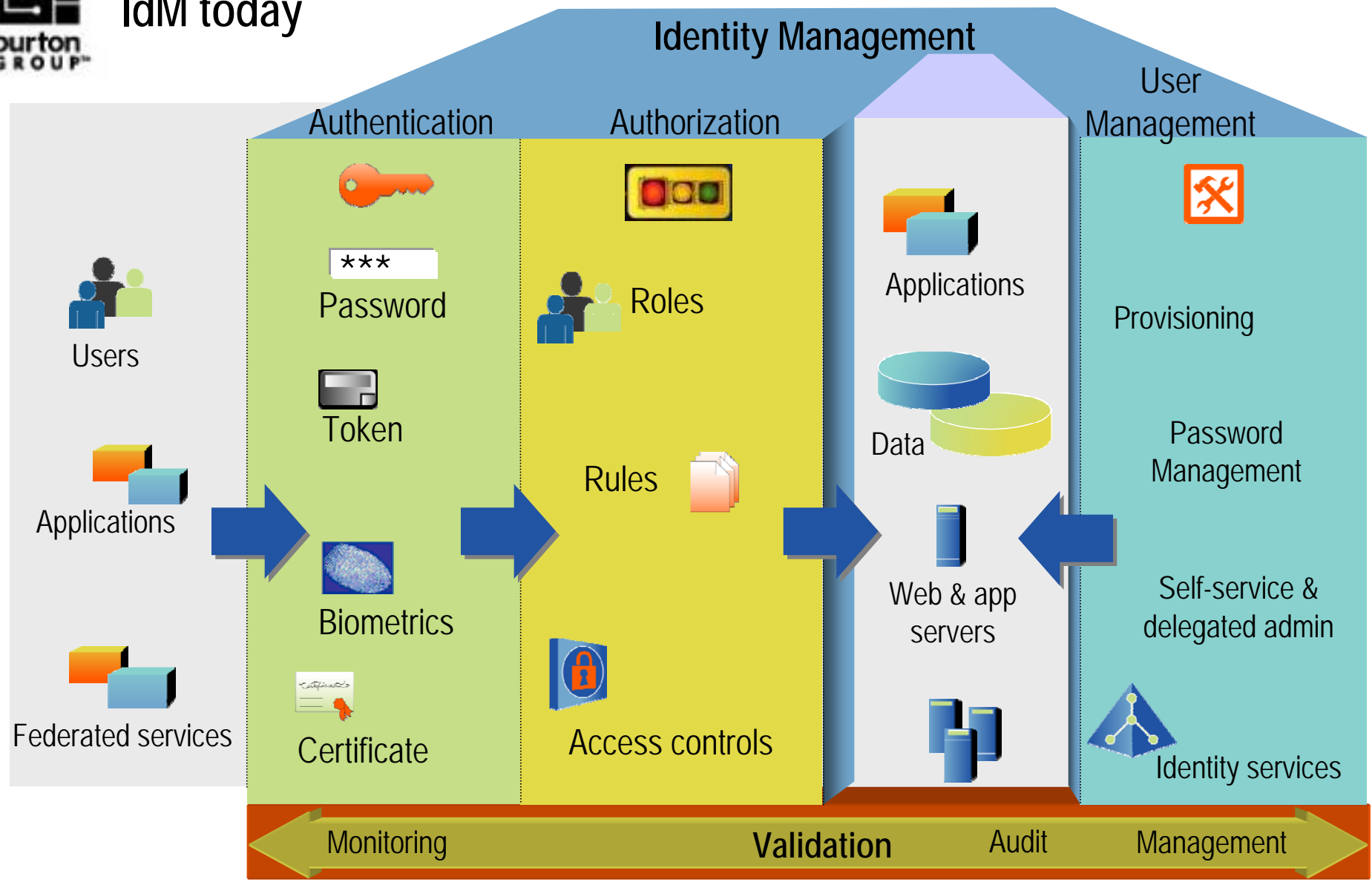
for the **creation, maintenance, and use**
of digital identities

in online spaces

Contemporary Control Systems



IdM today





Contemporary Control Systems

Identity management market directory

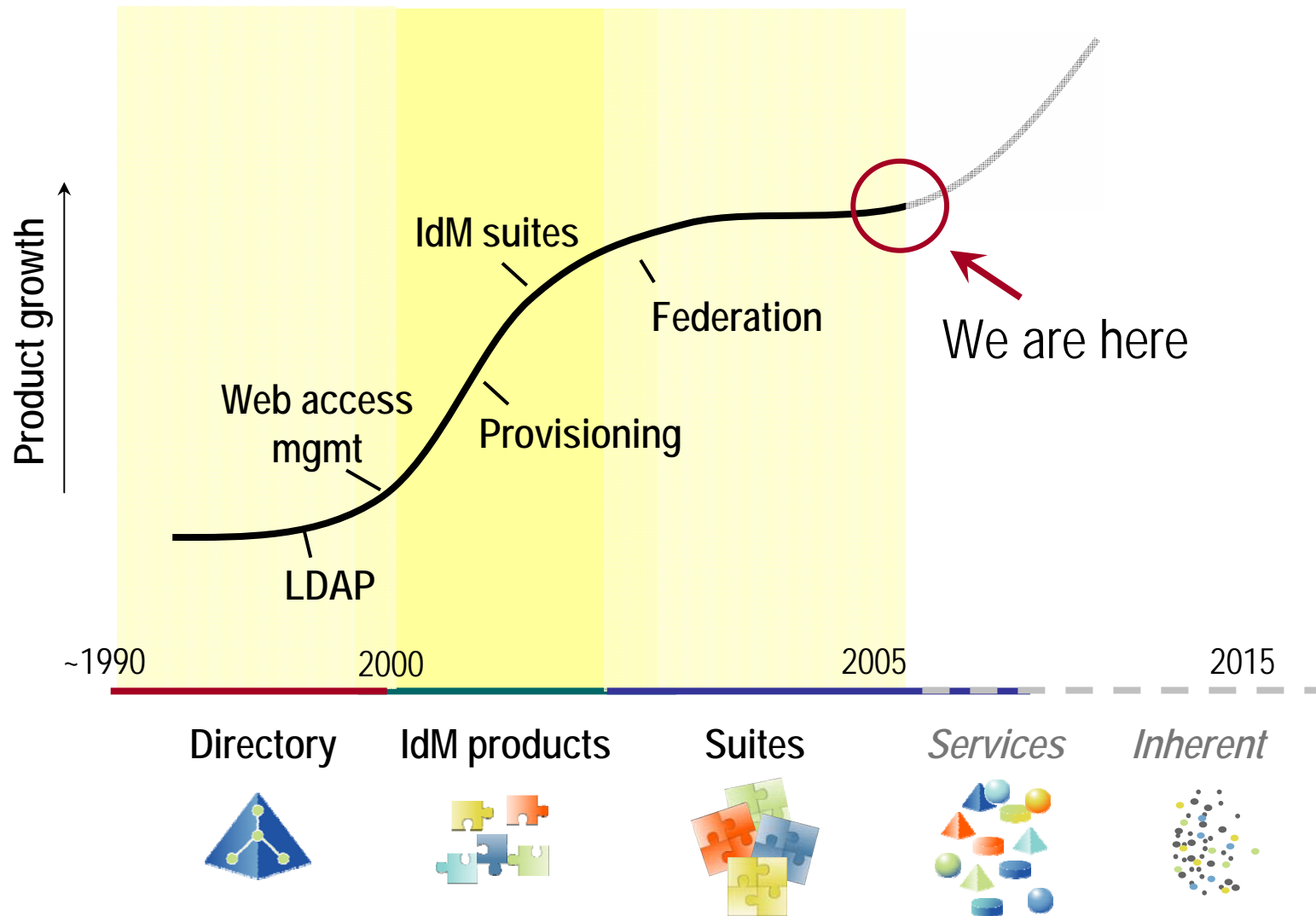
- Still over 60 vendors directly focused on IdM

ActivIdentity	Datapower	MaXware	Radiant Logic
ASG	Digital Persona	Microsoft	Red Hat
Authentify	Enatel	M-Tech	RSA Security
Avatier	Entegritiy	NetIQ	SafeStone
Axalto	Entrust	NetPro	Secured Serv.
Bayshore	Epok	NeuStar	Securent
BEA	Eurekify	Novell	Sentillion
Beta Systems	Evidian	OctetString	Siemens
BHOLD	Fischer Int'l	Oracle	Sun
BindView	Gemplus	OSM	Sxip
BMC	GlobalSign	Passlogix	Thor
BNX Systems	HP	Persistent Sys.	Valicert
Bridgestream	Imanami	Ping Identity	Veridicom
CA	Imprivata	Proginet	Voelcker
Citrix	Jericho Systems	Protocom	ZeroKnowledge
Courion	Juniper	Quest	Zkey
Credentica			

Contemporary Control Systems



IdM market progression at a glance



Contemporary Control Systems



The sound of things to come: rating the emerging trends

Noise Signal





Agenda

- The social context
- A look at contemporary control systems
- *What are other governments doing?*
- Revisiting the role of identity
- Recommendations



What are Governments Doing?

23

Governments are definitely moving on identity issues

- Differences across geographical/cultural boundaries
 - EU and Commonwealth efforts differ in approach from US efforts
- And projects address different needs, issues
 - Privacy protection, e-gov enablement, inter-agency interop, etc.
 - Privacy concerns have been different, but are starting to merge
- General observation
 - Many governments are realizing importance of federation
 - Multiple national and industry efforts to create trust frameworks



What are Governments Doing?

24

National ID cards: full of sound and fury, signifying something?

- United Kingdom
 - National ID card program has received lots of “attention”
- Belgium
 - Transitioning from paper ID cards to smart cards well under way
 - But the old one doesn't cost as much, so few people buy the new one
- Finland
 - National ID card (police station is RA) but not people or apps use it
 - Lottery company can use assertion from bank to buy your lottery ticket (may be proprietary)
- United States
 - RealID Bill makes driver's license the default national ID card
 - RFID-enabled passport regulations getting better, still problematic

What are Governments Doing?

25



Federated models are gaining traction

- United States
 - Federal PKI Bridge was the center, but now . . .
 - E-Authentication Framework, EAP Trust Framework
- Canada
 - Secure Channel Epass
- Europe
 - National ID card projects
 - Interest in federation in private, public sectors, many projects starting
 - Pan-European discussions on federation still at very early stages
- International, but industry- or community-specific
 - Shibboleth (higher education)
 - Visa CISP, BIO-SAFE, others: early trust frameworks, not federated yet

What are Governments Doing?

26



Some interesting analogs: Passports

- Reintroduced in 1914 with onset WWI
- International Conference on Passports, Customs Formalities, and Through Tickets (1920)
 - Under the auspices of the League of Nations
 - Issued standardization guidelines in 1920, more detail in 1926
 - US started requiring visas and passports for all aliens under the Immigration Act of 1924, impacted practices of other countries.
- 1944 Convention on International Civil Aviation (Chicago Convention), signed by the Allies, other UN members
 - Driven by problems with displaced persons during WWII, air travel
 - Required member states to develop, adopt international standards for customs and migration, including standards for passports



Some interesting analogs: Passports

- International Civil Aviation Organization (ICAO)
 - Established as UN body in 1946
 - Key role in developing standards to implement the Chicago Convention
 - Created the ICAO Panel on Passport Cards in 1968
 - ICAO Doc 9303 (1980) standardized entries in machine-readable passports (not all countries have implemented)
- US pushing Canada, EU to adopt RFID chips, biometrics
 - Most recent version of ICAO Doc 9303 includes standards for digitized biometric data encoded on a passport
 - But the RFID standards are still under development, so the US has attempted to impose its own

What are Governments Doing?

28



Some interesting analogs: Postal systems

- Bilateral postal treaties began in the 1500s in Europe
 - US proposed multinational convention in 1862 but Civil War interrupted
- 1874: Swiss convened Bern conference; 21 countries
 - Result: Treaty creating the General Postal Union (now the Universal Postal Union), second oldest international institution
 - UPU became a UN agency in 1948, now has 190 members
 - Check how long it took for majority to ratify UPU convention and join the system (you can get an idea by looking at the membership list, with dates of accession, at www.upu.int/members/en/members.html)



Agenda

- The social context
- A look at contemporary control systems
- What are other governments doing?
- *Revisiting the role of identity*
- Recommendations



Contemporary IdM systems and societal issues: a good fit?

- The design center for enterprise IdM is the domain
 - Organizational structure already exists
 - Clear ownership of resources
 - Administrators acts as facilitators and monitors
 - Bounded scope of use and reuse
- These assumptions don't hold true everywhere
 - What's the ID card for the societal context? or for the internet?
 - Who owns identifiers, attributes, and data?
 - Who has time and energy to manage everyone?
 - Who should be the admin, and who would monitor that admin?

Revisiting the Role of Identity

31



Fine grained authorization: An IT “justice zone”

- Where “it’s impossible to commit any act of injustice”
 - The ideal state is a very expensive proposition, likely not reproducible outside the lab
- Scaling authorization is extremely difficult
 - Especially when the input data is a CPR
 - Monitoring and auditing offer greater scale
- Structural solutions change users’ perception
 - From a collaborative problem to a facilitated / technical one
 - Strong identity = trust?





Revisiting the Role of Identity

32

Resources where socially cohesion is high are resilient

- Significant research in social sciences
 - Fisheries, water basins, irrigation systems
- Emerging online corollaries
 - Wikipedia
 - Open source projects
 - eBay reputation
 - Blogs and comments
 - Commercial e-mail sites and spam filtering
 - Commercial instant message applications
 - Standards committees
 - Social networks
- User-centric identity systems



Fostering collaboration

Appropriators are active participants in creating the dilemmas that they face, and under certain conditions, if given the opportunity, active participants in resolving them. They are not inevitably or hopelessly trapped in untenable situations from which only external agents can extricate them.

— E. Schlager



Revisiting the Role of Identity

34

Conditions improving the chances of spontaneous collaboration

- Ostrom theorized that six conditions improve chances
- This audience may fit these “entrance requirements”
 1. The appropriators perceive they will be *harmed* in some way if no action is taken
 2. A *fair solution* can be found through which all appropriators will be affected in similar ways by the rules
 3. The *durability* of the relationship is believed to be high (low defection rates among appropriators)
 4. The *cost* of participation is reasonably low
 5. Most appropriators share social *norms* of reciprocity and trust
 6. The group of appropriators is *stable* and, preferably, *small*
- Example: West basin in California



Revisiting the Role of Identity

35

Theory of common pool resource management (Ostrom)

1. **Exclusion** – The group must be able to guard the resource from free loading, theft, or vandalism.
2. **Rationality** – The agreed upon rules must be attuned to the context of the resource
3. **Involvement** – Members have avenues to participate in modifying operational rules
4. **Monitoring** – Effective monitoring and auditing or policies
5. **Enforcement** – Sanctions can be imposed on violators of the rules
6. **Arbitration** – Appropriators have access to low cost, but effective conflict resolution
7. **Autonomy** – The rights of appropriators to devise their own institutions



Facilitating collaboration

- “Good fences make good neighbors” (R. Frost)
 - Exclusion is important, but fences in virtual, distributed space are problematic; identity is a handy post for virtual fences
 - “Exclusion, while critical, is insufficient to ensure long-term commitment to the rules” (E. Schlager)
- How then to maintain social order?
 - “The foundation of cooperation is not really trust, but the durability of the relationship” (R. Axelrod)
- Durability of relationship requires recognition
 - But not a necessarily high degree of identity vetting or authentication



Revisiting the Role of Identity

Evolution of identity in cooperative relationships

<u>Today</u>		<u>Next generation</u>
Identity	→	Relationship
Identification	→	Recognition
Domain	→	Community
Control	→	Collaborative action
Privilege	→	Reputation
User	→	Participant? Contributor?



Agenda

- The social context
- A look at contemporary control systems
- What are other governments doing?
- Revisiting the role of identity
- *Recommendations*



Recommendations

39

The 7 flaws of identity: avoiding hamartia in the architecture

- Believing identification makes things more secure
 - Identification can improve security, but it's not the inevitable outcome
 - But over-identification has repercussions on privacy
- Ignoring unintended consequences (externalities)
 - Real problems (like ID theft, fraud) need real solutions
 - But let's try not to create new ones while solving 1st order problems
- Forgetting that use of a system invites abuse of it
 - Need to test the architecture with attack vectors
- Allowing the weakest links to lead to catastrophe
 - Smart cards don't prevent social engineering and insider attacks
 - Encrypting the channel doesn't stop dumpster diving

The 7 flaws of identity (cont'd)

- Insisting every dilemma nail requires the identity hammer
 - Identity should be used with caution, sparingly



- Mistaking the identity for the relationship
 - Technology should support natural social constructs
- Believing there are only 7 flaws
 - But IdM empowers organizations to flourish, so worth the trouble!



Conclusion

- Traditional methods of social order are problematic
 - Don't scale well and are inherently non-social
- A canon of research supports a new approach
 - "Evidence suggests that governments may be of greatest benefit to appropriators by providing a supportive environment that encourages appropriators to devise their own solutions to the dilemmas that they face."

— E. Schlager
 - Optimizing the environment for the administrative view is usually a suboptimal configuration
- Technology must therefore support social processes of recognition, group awareness, reputation, and reciprocity