Biometrics as 'RegTech'?

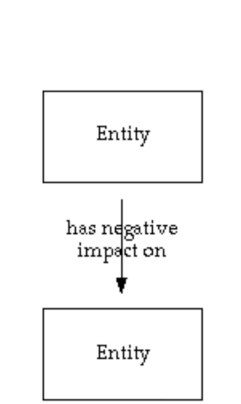
Roger Clarke

Xamax Consultancy Pty Ltd, Canberra
Visiting Professor, UNSW Law
Visiting Professor, Research School of Computer Science, ANU
Board-Member, Australian Privacy Foundation

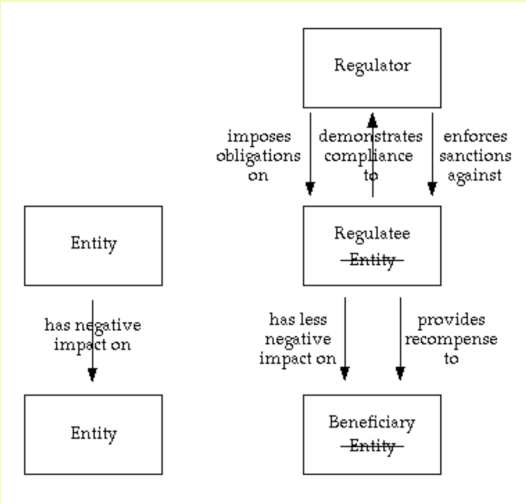
http://www.rogerclarke.com/ID/BiomReg {.html, .pdf}

SINS17 – Sydney – 9 August 2017

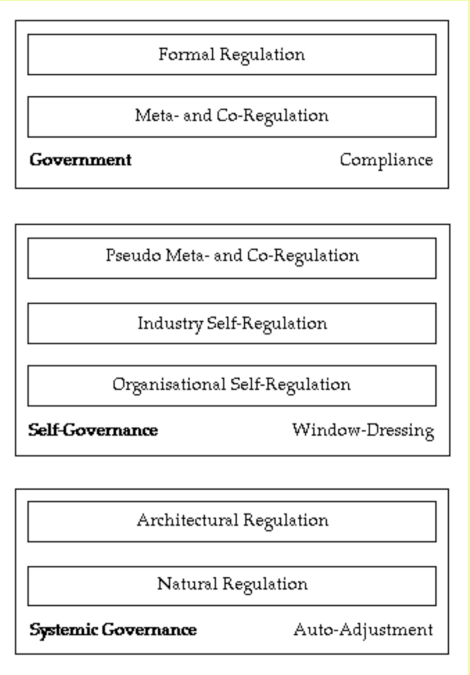
The Motivation for Regulation



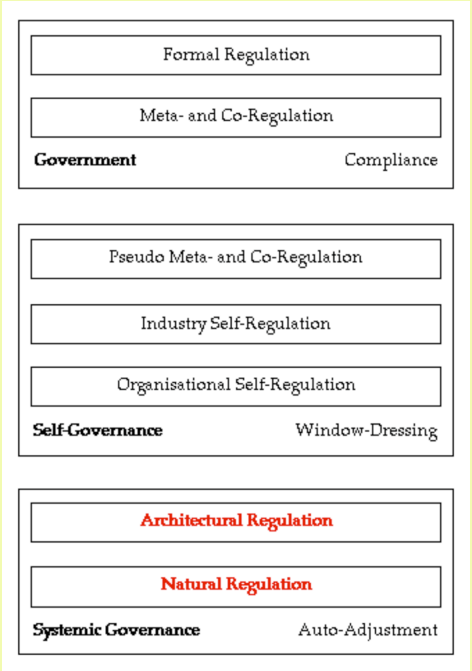
The Players in the Regulatory Scheme



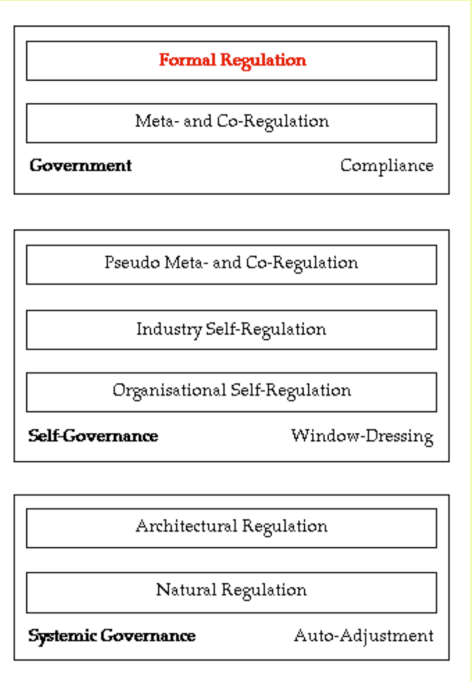
The Layers of Regulatory Mechanisms



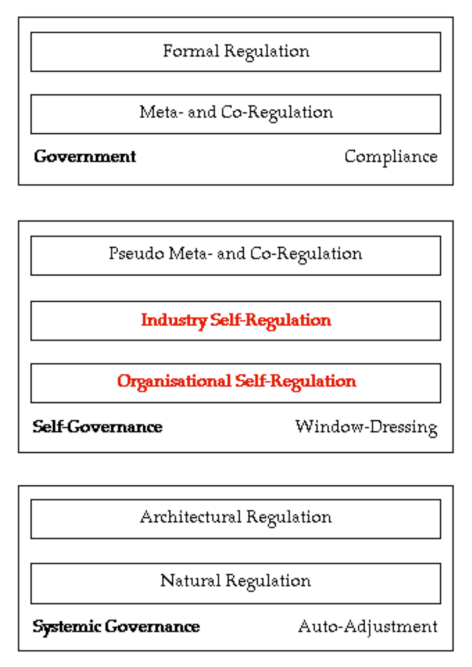
The Layers of Regulatory Mechanisms



The Layers of Regulatory Mechanisms



The Layers of Regulatory Mechanisms



RegTech

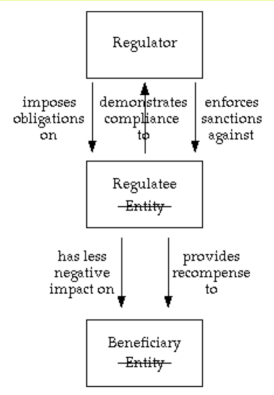
'Use of Technology
to reduce compliance costs
arising from the Regulation of financial services'

RegTech

'Use of technology to reduce compliance costs in financial services'

Application of **Tech**nology to <u>any</u> aspect of **Reg**ulation, for <u>any</u> player, in <u>any</u> regulatory scheme, incl.:

- regulatees ('compliance')
- regulators
- intended beneficiaries of regulatory activity



Some Examples of RegTech

For Regulatees

- Access control
- Audit trails
- Automated monitoring of accesses
- Incident management
- Automated statistical reporting
- Baseline IT and data security measures
- Complaints-handling

itnews

CBA accused of aiding fraud with intelligent deposit machines

By Ry Crozier
Aug 3 2017
4:15PM

Faces civil suit filed by AUSTRAC.

0 Comments

The Commonwealth Bank has been accused of deploying a fleet of intelligent deposit machines without effective fraud controls, enabling $77 million of suspicious transactions to be made using the machines over a three year period.

Financial regulator AUSTRAC has filed civil proceedings against the bank in the Federal Court, alleging over 53,700 contraventions of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act).

https://www.itnews.com.au/news/cba-accused-of-aiding-fraud-with-intelligent-deposit-machines-470058

CommBank Statement 7 August 2017

CommonwealthBank

- ... the issue **began in late 2012 ... when a coding error occurred** [sic – was made] that meant the machines didn't create the threshold transaction reports needed
- ... the error **became apparent in 2015 – ?!**
- Austrac was **notified within a month** of [the discovery], the missing reports were provided and the coding error fixed
- the vast majority of the reporting failures alleged by the agency, about 53,000, relate specifically to the coding error
- [however, **the Bank] recognizes other serious allegations** were also made by Austrac

https://www.cmcmarketsstockbroking.com.au/stockdetails/News/StockNewsStory.aspx?storyid=20170806DN001207

Some Examples of RegTech

For Regulatees

- Access control
- Audit trails
- Automated monitoring of accesses
- Incident management
- Automated statistical reporting
- Baseline IT and data security measures
- Complaints-handling

For Regulators

- Financial transactions tracking
- Real-time transactions monitoring
- Audit trail analysis
  (e.g, in health, for fraudulent invoicing, over-servicing and doctor-shopping)

Some Examples of RegTech

For Regulatees

- Access control
- Audit trails
- Automated monitoring of accesses
- Incident management
- Automated statistical reporting
- Baseline IT and data security measures
- Complaints-handling

For Regulators

- Financial transactions tracking
- Real-time transactions monitoring
- Audit trail analysis
  (e.g. in health, for fraudulent invoicing, over-servicing and doctor-shopping)

For Beneficiaries

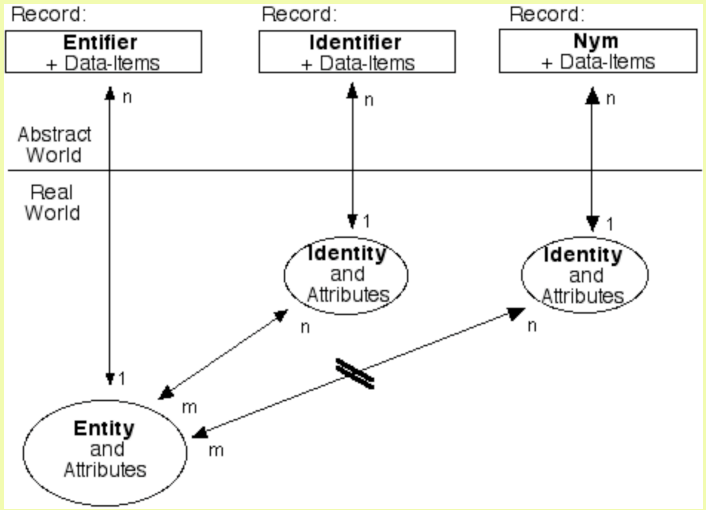
- Guidance on dealing with miscreant organisations
- A portal enabling discovery of relevant regulators and complaints-handlers
- A wizard to check for a right to complain
- Wizards for initiating formal complaints

Identity 'Provisioning' and 'Management'

- A longstanding presumption that identity, particularly of people, is central to social control

http://www.rogerclarke.com/DV/HumanID.html
http://www.xamax.com.au/EC/IdMngt.html

(Id)Entifiers and (Id)Entification



http://www.rogerclarke.com/ID/IdModel-1002.html

Identity 'Provisioning' and 'Management'

- A longstanding presumption that identity, particularly of people, is central to social control
- Can biometrics help?

http://www.rogerclarke.com/DV/HumanID.html#Bio
http://www.rogerclarke.com/DV/Biometrics.html
http://www.rogerclarke.com/DV/BiomThreats.html
http://www.privacy.org.au/Papers/Biometrics.html
http://lockstep.com.au/blog/biometrics

Identity 'Provisioning' and 'Management'

- A longstanding presumption that identity, particularly of people, is central to social control
- Can biometrics help?
- Arner et al. propose the 'India Stack' for RegTech. Its base is "a national system of biometric id"

AADHAAR
Unique Identification Authority of India

Arner D.W., Barberis J. & Buckley R.P. (2016)
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847806

http://uidai.gov.in

Identity 'Provisioning' and 'Management'

- A longstanding presumption that identity, particularly of people, is central to social control
- So can biometrics help?
- Arner et al. like the 'India Stack' for RegTech, whose base is "a national system of biometric id"
- **Aadhar is subject to current legal action for breach of the constitutional right to privacy**

Greenleaf (2016) – https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800835

Questions the Biometrics Industry Avoids

- Are biometric technologies **effective?**
- Whether or not biometric technologies are effective, are they so inherently privacy-invasive that their use is **inimical to human rights and democracy?**
- If biometric technologies are reconcilable with human rights, **what design principles** must be rigorously imposed on them and their application?

'Factors Affecting Performance'
(Mansfield & Wayman, 2002)

- **Demographics** (youth, aged, ethnic origin, gender, occupation)
- **Template Age**
- **Physiology** (hair, disability, illness, injury, height, features, time of day)
- **Appearance** (clothing, cosmetics, tattoos, adornments, hair-style, glasses, contact lenses, bandages)
- **Behaviour** (language, accent, intonation, expression, concentration, movement, pose, positioning, motivation, nervousness, distractions)
- **Environment** (background, stability, sound, lighting, temperature, humidity, rain)
- **Device** (wear, damage, dirt)
- **Use** (interface design, training, familiarity, supervision, assistance)

http://face-rec.org/databases/mansfield02.pdf

Are biometric technologies effective?
Technical 'Features'

- **Significant Non-Capture Rates** ('failure to enroll'), necessitating:
- **Problematical Exception-Handling Processes** at both registration points and operational locations where business processes depend on biometric capture
- **Material Inconsistency of Capture** and the inherent fuzziness of biometric measures, which results in:
- **Dependence on Fuzzy Matching** of new measures against reference measures, which necessitates:
- **Thresholds**, often arbitrary thresholds, **for acceptance / rejection of assertions**
- **High False +ive +/or False -ive Scores** i.e. mistakes, resulting in:
- **The Necessity to Trade Off Between Aims** with the result that:
- **Security Objectives are Compromised by Operational Exigencies**, plus:
- **More Problematical Exception-Handling Processes**, some inevitably informal and uncontrolled workarounds, resulting in:
- **Low Credibility of Schemes** not least with the people who operate them
- **Lack of Speed**
- **Lack of Scalability**
- A wide array of **'Failure Modes'**
- **High Vulnerability to Attacks** by parties with a motive to defeat the system
- **High Risk of Masquerade / Id Fraud** ("a person's biometrics aren't a secret")

Are biometric technologies effective?
Socio- 'Features'

Intrusiveness into:

- **Privacy of the Physical Person**
- **Privacy of Personal Data**
- **Privacy of Personal Behaviour** esp. freedom of speech, thought
  Chilling arises whether or not the system works, whether or not the behaviour is the kind intended to be chilled

Strong Links With Authoritarianism

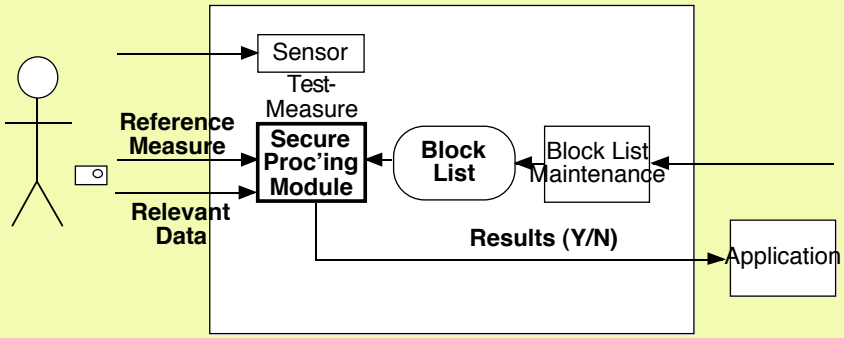
Products are intended to be repressive, are designed for unfree countries, are retrofitted into nominally free nations

Public Acceptability

When publicised, negative impacts on acceptance, adoption, corporate reputation and government agency trust

http://www.rogerclarke.com/DV/Biometrics.html#Thr
http://www.rogerclarke.com/DV/BiomThreats.html#ImpImp

Privacy-Sensitive Architecture
e.g. Authentication Against a Blacklist



http://www.rogerclarke.com/DV/BioArch.html (2002)

Biometrics as RegTech

(1) Directors of Phoenix Companies

The Aim

- Restrict the use of an identifier to only one person
- Force them to use it when they act as a director
- Prevent them acquiring more than one identifier
- Find, prosecute and sue each person whose identifier is linked to an offence
- Preclude them from being a company director

A Biometric Scheme to Achieve The Aim

- Require **registration** with ASIC or its (managed) agent
- Capture their **biometric measures** into the Register
- Search for match(es) already in the Register (**Entification**)
- Require further capture of their **biometrics as a condition of conducting specified activities**
- Compare that with the previously-recorded measure **(Entity Authentication)**
- **Criminalise** refusals and attempts to subvert the scheme

A Biometric Scheme to Achieve The Aim

- Require **registration** with ASIC or its (managed) agent
- Capture their **biometric measures** into the Register
- Search for match(es) already in the Register (**Entification**)
- Require further capture of their **biometrics as a condition of conducting specified activities**
- Compare that with the previously-recorded measure **(Entity Authentication)**
- **Criminalise** refusals and attempts to subvert the scheme

2.5m Aust. corps, 250-500,000 company director identities

Of those, 11,500 corporations and 2,500 directors are suspects

The scheme affects 100% of them, not just the **0.5-1.0% suspects**

Biometrics as RegTech

(2) The Management of Data Access

The Aim

- Protect sensitive data from unauthorised access

Australian Government
Medicare Australia

medicare

A Current Context

- Medicare Registry data is accessible by > 200,000
- The data is a goldmine for Id Fraud
- Access control is very lax; the system is large; safeguards and controls appear to be very limited

A Biometric Scheme to Achieve The Aim

- Enhance >100,000 **devices** capture biometrics
- Require >200,000 staff to go to (Centrelink?), register, **provide a biometric, receive an authenticator, not lose it**, and never leave it at home or at the wrong workplace
- **Enforce entification** for logon & key transactions
- **Prevent subversion**, by enforcing short time-outs before requiring the user to re-authenticate
- Cope with **a (say, trebling?) of users** and a substantially more onerous and slower registration process

A Biometric Scheme to Achieve The Aim

- Enhance >100,000 **devices** capture biometrics
- Require >200,000 staff to go to (Centrelink?), register, **provide a biometric, receive an authenticator, not lose it**, and never leave it at home or at the wrong workplace
- **Enforce entification** for logon & key transactions
- **Prevent subversion**, by enforcing short time-outs before requiring the user to re-authenticate
- Cope with **a (say, trebling?) of users** and a substantially more onerous and slower registration process

Better, because less masquerade
Worse, because far more people are authorised
Hence a moderate **increase** in the data's vulnerability

Biometrics and 'RegTech'

AGENDA

1. Regulation
2. RegTech
3. Biometrics
4. Biometrics as a Form of RegTech
   (1) Pheonix Company Directors
   (2) The Management of Data Access

Messages

- Before considering biometrics, it's crucial to **know what the problem is** that you're trying to solve
- **All biometric schemes face big technical challenges, and must handle multiple exception-conditions** esp. where the context involves large volumes of transactions, multiple failure-modes, or adversaries
- At some stage, **the real nature of the scheme, and its shortfalls, will both become publicly obvious, and it will incur intense dislike** among many people
- **Those affected have the power to cause you grief**

Process Guidelines

- **Evaluate calmly and realistically**
  and avoid getting caught up in supplier hype
- **Avoid cartels of users-and-providers**
  The Biometrics Institute harms the shareholders of companies that get sucked into spending money on ineffective technologies
  This "user group with a majority of user members", is 42% user organisations, 50% supplier members (July 2017)
- **Evaluate using the meta-principles**

1. Evaluation 2. Consultation 3. Transparency 4. Justification
5. Proportionality 6. Mitigation 7. Controls 8. Audit

Biometrics as 'RegTech'?

Roger Clarke
Xamax Consultancy Pty Ltd, Canberra
Visiting Professor, UNSW Law
Visiting Professor, Research School of Computer Science, ANU
Board-Member, Australian Privacy Foundation

http://www.rogerclarke.com/ID/BiomReg {.html, .pdf}

SINS17 – Sydney – 9 August 2017