

Goldfish come round again

Adrian R D Norman

*(Discussion paper for the EURIM: Directors' Round table
on Information Governance; November 2008)*

Abstract

This paper focuses on the regulation of computerised identity services on the world-wide web and its successors. The science of Cybernetics shows that an effective regulatory system must develop as fast as the increases in volume and variety of the system it regulates. Since the technology of the information systems used by the identity services has been growing exponentially in capability for 50 years and shows no sign of slowing down, government regulation cannot work. Furthermore, identity systems and the threats they face are inherently international and governments are unlikely to reach agreement on regulation quickly.

Thirty years ago, when PCs and the internet were a future prospect, computers were 30,000 times less powerful and more than 1,000 times rarer. When the author described the concept of a Global Data File in an Information Systems Haven as an identity service provider, the world's stock of IT was at least 30 million times less than today.

The knaves and fools can quickly tap the increasing power of IT to find weaknesses in ID systems to steal and lose data. If one succeeds, the monopolist loses the trust of its clients and so does the regulator; at present both are government.

So when the goldfish come round yet again, this paper calls for a shoal of ID service providers with an independent regulator. The worldwide market is a better regulator of the performance of service providers than a government official. The official is essential to regulate integrity.

What is the question?

The organisers' have brought us together to consider questions¹ from which the following is an abstract:

The time has surely come to rebuild confidence around regulation that is
based on practical experience, rather than legal or political theory.
But how can and should good practice be identified, fostered and enforced?
How much is about people processes rather than technology?

This paper argues for regulation based on proven scientific laws since experience shows that man-made laws will fail if they mandate the impossible.

No one can have practical experience of the future but it is possible to have experience of predicting the future.

It is 40 years since James Martin and I wrote "The Computerised Society"² and 25 years since I published "Computer Insecurity". The former looked ahead 15 years to 1984; the latter looked back over the history of computers. Since it82 and the first Data Protection Act, we have seen about three generations of IT in one human generation. Regulation of computing and liberalisation of telecommunications came with their convergence at the start of the 80s. Since then, regulators have been regularly surprised that the past is not a reliable guide to the future³. Some of the problems raised and the solutions provided by successive generations of IT are unprecedented.

The agenda is driven by technology and cannot be changed by the human successors to Canute's courtiers. Confidence cannot be rebuilt on *will* to do the impossible. There is nothing more impractical than to attempt the theoretically impossible.

Restatement of the question

Is there a *will* ... to take a lead ... in rebuilding their information governance systems so that they inspire confidence among those concerned that they are fit for purpose.

This raises further questions:

What is the objective?

Who are those concerned?

How do we assess fitness for purpose?

How does a system inspire confidence, or conversely ... loss of confidence?

Why the question is being raised now?

The issue was being discussed more than 40 years ago. "The Computerised Society" addressed it and proposed protective action. So did the Privacy and Public Welfare Committee of the BCS on which I served in the 70s. The BCS paper in this series⁴ and I concur with their analysis of the problem.

Essentially there are three reasons for the present political interest:

1. *Data loss*. There is media interest because the data are personal and public interest in media reports⁵, Media interest engenders political interest.

2. *Data sharing plans and joined-up systems*. The stock market crash in 1987 was caused by the sharing of data and joining up of systems in the international money centres in the previous decade. This time, the whole economy is joined up. People fear joined up governments with power to regulate travel and migration.

3. *Criminal opportunity and activity*; Falstaff⁶ has his answer: a commodity of good names is to be found on the worldwide web! Ultimately, there will be a collection of 7 billion IDs, each associated with its unique DNA, the fundamental biometric which distinguishes individuals but also links them through inheritance: the ultimate discriminator.

How access to personal records can be regulated

Regulation has a scientific foundation: cybernetics. It calls for an objective, a measurement of deviation from the objective and a means of correcting the deviation. When regulating risk, the challenge is to define the multi-dimensional objective function.

Cybernetics and government

The theory of government and regulation, *cybernetics*, is derived from the Greek for steersman (gubernator). Its laws underpin information theory, information science and hence the information technology on which information systems are based.

Government information systems are both part of the regulatory system and a system in need of regulation, making them inherently difficult to analyse. Furthermore, they are not only designed independently and continuously evolving, they are of different ages and interact in ways not anticipated by their designers. In particular, they involve both negative and positive feedback control systems by design and by default.

Negative feedback measures the extent of deviation from the intended course and applies a proportionate force to bring it back (e.g. the Monetary Committee). It leads to waves such as economic cycles, seasons and tides. The equations of motion of a pendulum, the planets and other cyclic systems have solutions in which the exponent is an imaginary number.

Positive feedback measures the stock and grows proportionately. The exponent is a real number and results in exponential growth. The Australian experience of exotic creatures like cane toads and rabbits exhibits exponential growth. Achieving the goal of macro-economic policy, year on year

growth in GDP of several per cent, relies on positive feedback. Like global warming, real world examples of positive feedback end in disaster. As a nuclear physicist at Aldermaston, I was conscious of the difference in **effect** between uncontrolled bombs (positive feedback) and controlled reactors (negative feedback).

The theory: Ashby's Law

An information system which is part of a regulatory system is bound by Ashby's Law⁷, which is fundamental to information science. "Only variety can control variety". If you cannot discriminate between people, you cannot treat them differently.

The observed behaviour: Moore's Law

Unfortunately, Ashby's Law co-exists in practice with the observed growth in performance of information technology: Moore's Law⁸. Fundamentally, the exponential growth in performance of IT systems arises from the fact that IT systems are used to design and build IT systems; the better they are the faster they get better - an example of positive feedback. The information economy differs in this respect from the industrial and agricultural economies that preceded it.

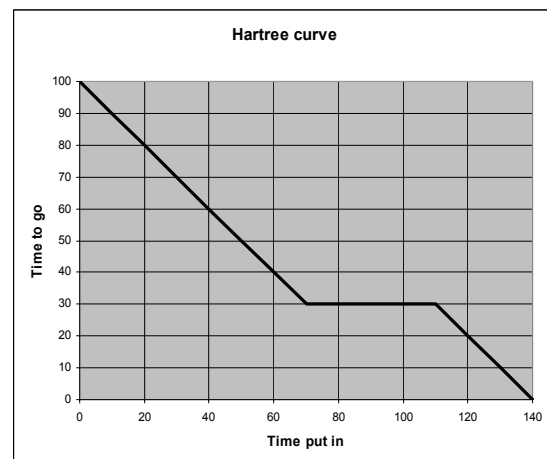
Over time, regulatory systems that obey Ashby's law have to grow in line with the variety and performance of the systems they regulate. If they are regulating information technology systems, then the speed and variety are growing exponentially and will inevitably outstrip the regulatory capability of any control system that does not develop as fast. The reaction times associated with international treaties (ca. 20 years), national legislation (ca. 10 years), trade association guidelines (ca. 5 years), corporate policies (ca. 3 years), all of which require agreement among people, are too long for effective regulation. At the leading edge of business and crime, some innovations take just months.

Who regulates the regulators that design, build and operate the regulatory system? This brings to mind Gladstone's unsolved problem as described in *1066 and all that* – the Irish changed the question⁹ whenever he answered it.

Systems in the real world: Murphy's law and Hartree's law

Unfortunately, two other 'laws' apply: Hartree's and Murphy's. Both are empirical, being based on observations of the real tangible world. Murphy is mythical but strikes a chord by noting that "if it can go wrong, it will". D R Hartree was a pioneer of computers to whom this curve is attributed.

When you start, you do not know all the problems to be solved. By the time you do, it is impossible to finish by the contracted delivery date. The winner's curse applies to systems procured by government: "If you bid low enough to win the contract, you will lose money on the project", partly because you did not factor in the Hartree plateau.



Systems in the intangible world

We are talking about governance systems for the intangible world in which, for example, the conservation laws underlying classical economics do not apply. You can sell information and still have the use of it, which is not the case with bread or cars.

Progress up the hierarchy of data, information, knowledge and wisdom over the last 50 years is reflected in the names we used: electronic data processing, information technology and the knowledge economy. (We have yet to achieve wisdom).

In the 1970s, the CCTA and the GPO provided government EDP and telecommunications. Now this infrastructure is outsourced to the private sector, a significant part to foreign owned businesses.

British suppliers were slow to offer world-leading IT products and services to foreign governments because HMG did not ask for them.

In the knowledge economy, we are going the same way. Instead of calling for services that meet world needs and using them itself, government procures to a specification based on its own needs. So we will [continue to](#) import more than we export.

Imaginary systems in the real world

“Project Goldfish”

*Computer Insecurity*¹⁰ was published about the same time as the first Data Protection Registrar was appointed. It included a spoof consultant’s feasibility study of “Project Goldfish”, originally published¹¹ in 1978. The brief was to examine the technology and market for a *Global On-Line Data-File in an Information Systems Haven* where international regulations on data protection did not apply. Goldfish was presented to the first conference on TransBorder Data Flows. Among the delegates were lawyers and officials who thought that they could repeal the laws of physics. TBDFs raised the issues of extraterritoriality which Goldfish exposed and which remain unresolved. The internet provides havens for information systems that governments wish to suppress or regulate, including those gathering personal data like Goldfish, which is why it comes round again now.

The limits to growth are not set by the number of people in the world but by the number of relationships between natural and legal persons that someone may want to record. Linking records in identity databases has been essential to the spread of genealogy as a hobby. When an individual’s unique DNA is added, family trees will be traced automatically and the sins of the child will be visited on the father, whether or not the relationship had the benefit of clergy.

Unless the UK creates better systems than Goldfish, some other country will do so, and realise the economies of scale, eventually exporting services to British citizens in the way we export “invisibles” profitably today.

The practical limits to regulation

Having shown what regulators cannot do, what remains that is both possible and desirable?

We need to:

- put a trusted barrier between the data store and those who wish to use and distribute its contents;
- have many competing service providers so that innovation is constant; and
- engender trust at home and abroad.

We can achieve this by developing electronic stewardship provided by competing businesses regulated by government and the market.

The electronic steward

It was the 18th century practice to employ a steward to look after your affairs, if you could afford him. We can all afford one now thanks to advances in IT.

The e-steward would be answerable to, and compete for, a citizen’s business, as with motor insurers today. Regulated by government and the market, the identity service provider must gain and retain the trust of both its clients and its overseers for two services: identity and custody.

The identity service identifies individuals from their attributes on receiving a lawful request, but does not disclose irrelevant attributes or information about individuals not meeting the profile. It provides the pertinent subset of stored attributes if the subject instructs his e-steward to release them e.g. for job applications or tax returns.

The custody service checks the client's biography and biology by biometry and by cross-checking claims. It vouches for accuracy of verifiable claims in a CV, for example. It holds the relevant part of the Population Health Index, providing routine and emergency data when needed. It keeps metadata which says who has seen what and under what authority.

The regulator of e-stewards ensures that it is simple to change from one to another if dissatisfied with the service, if a better service is available from a competitor or the service is taken over. Different architectures and levels of service mean greater immunity to common mode failure.

All e-stewards implement the Kim Cameron's Laws of Identity¹²

- 1 User Control and Consent
- 2 Minimal Disclosure when required
- 3 Justifiable Parties
- 4 Directed Identity
- 5 Pluralism of Operators and Technologies
- 6 Human Integration
- 7 Consistent Experience Across Contexts

In place of a vulnerable National Identity Service, the time has come to scatter the convoy¹³ to increase probability of survival. Different architectures and software can be used to achieve same ends so it is unlikely that knaves and fools can breach the security of several stores, let alone all of them at once. Successful defences can be disseminated quickly.

The value of good regulation

Trust is an exportable service in the global knowledge economy. National governments are not trusted to provide trust services, but some of the 200 or so would be trusted to regulate trust service providers.

Contrast the trusted services that our e-stewards could provide before, during and after the 2012 Olympics to athletes, officials and visitors from around the world with what the Chinese could have offered this year. We would put the data subject's need for security and privacy ahead of the state's need for control.

If the service from UK e-stewards is good enough for the British, foreigners will want it. Our invisible exports show what we can do with well regulated corporations operating in competitive markets. But it is also clear that the regulators have to understand how information technology affects both the regulated and the regulatory systems. The past is a poor guide to the future.

End notes

¹ See the calling notice at: <http://www.eurim.org.uk/activities/ig/drt081124.php>

² The Computerised Society, by James T. Martin and Adrian R D Norman, Prentice Hall, New Jersey, USA 1970 ISBN 140215581

³ See for example Black-Scholes formula: an option's future value depends on the past volatility of the underlying assets

⁴ The papers available before this were:

Louise Bennett (BCS), *Information Governance - Responsibilities for personal data holdings*

Len Anderson (SOCITM) *Information Governance for Sharing Personal Data*

Tim Boswell MP & others, *Motion for a Resolution to the Council of Europe Parliamentary Assembly: Identity Documents & Databases*

Paul Wilson (De La Rue), *The Information Agenda*

Carlos Solari (Alcatel Lucent), *The Will to Regain the Confidence - Trust of Our Customers & Citizens*

CSC, *Secure Data - A Government Challenge*

Andrew Hardie, *Information Governance – Just Say No*

⁵ Such as the BBC's calculation that the government had lost personal data on four million citizens in FY 2007/8

⁶ "I would to God thou and I knew where a commodity of good names could be bought."
Falstaff, Henry IV Pt1, 1, ii-

⁷ Ashby's Law of Requisite Variety: variety absorbs variety, defines the minimum number of states necessary for a controller to control a system of a given number of states. W. Ross Ashby (1956): *An Introduction to Cybernetics*, (Chapman & Hall, London) – available electronically at <http://pcp.lanl.gov/ASHBBOOK.html>

⁸ Moore's law describes a long-term trend in the history of computing hardware. Since the invention of the integrated circuit in 1958, the number of transistors that can be placed inexpensively on an integrated circuit has increased exponentially, doubling approximately every two years

⁹ *1066 and All That*, Sellar and Yeatman's humorous book on British history, was first published in 1930. What they actually wrote was 'Gladstone spent his declining years trying to guess the answer to the Irish question; unfortunately, whenever he was getting warm, the Irish secretly changed the question.'

¹⁰ Computer Insecurity by Adrian R. D. Norman, ISBN 412223104, London : Chapman and Hall 1983

¹¹ 'Project Goldfish' article in Information Privacy, Sep 1978. IPC Business Press, Guildford
<http://www.adminet.co.uk/clients/ANAAL/goldfish.pdf>

¹² Kim Cameron, Architect of Identity, Microsoft <http://www.identityblog.com/?p>

¹³ Convoys in WW2 came together for mutual protection e.g. against submarines by concentrating firepower, sharing of escorts; but were easier to locate by aircraft, went at the speed of the slowest, and were vulnerable to attack by capital ships with longer range guns. In the Vietnam War the Americans lost to the Viet Cong, who did not concentrate their forces. In the American War of Independence the rebels did not stand and fight till Cornwallis was unable to bring in reinforcements.