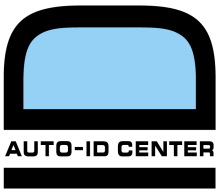
Published February 1, 2003. Distribution restricted to Sponsors until May 1, 2003.



EXECUTIVE BRIEFING

Options for Regulation of the EPC™ Network

Kevin Ashton

AUTO-ID CENTER MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 400 TECHNOLOGY SQUARE, SIXTH FLOOR, CAMBRIDGE, MA 02139-4307, USA

ABSTRACT

New technology can scare people. As the Auto-ID Center introduces its new technology, people around the world will seek assurance that neither they nor their rights are threatened. Unless this assurance can be made and is believed, the technology may fail.

Over the past two years, the Center has conducted extensive research to understand public response to its technology, including focus groups and expert interviews in five countries. The reactions can be summarized as 'neutral to negative'. People are willing to accept the technology if, and only if, they can be confident there is appropriate protection from risk and abuse. Privacy rights and health protection are most often cited as areas where reassurance is necessary.

This paper discusses how such reassurance could be provided. It is not a proposal or a strategy, but rather is intended to frame, aid and inform constructive discussion. As such, it does not represent an agreed policy of the Auto-ID Center, the Massachusetts Institute of Technology, or any person or organization affiliated with the Auto-ID Center, either explicitly or implicitly. It is a discussion document, and nothing more.

Published February 1, 2003. Distribution restricted to Sponsors until May 1, 2003.

EXECUTIVE BRIEFING

Options for Regulation of the EPC™ Network

Biography

Kevin Ashton
Executive Director

Kevin Ashton is Executive Director of the Auto-ID Center. He is on loan to the Massachusetts Institute of Technology from the Procter & Gamble Company. He is a graduate of University College London, and a Visiting Engineer in MIT's Department of Mechanical Engineering.

EXECUTIVE BRIEFING

Options for Regulation of the EPC™ Network

Contents

1. INTRODUCTION

New technology can scare people. As the Auto-ID Center introduces its new technology[1], people around the world will seek assurance that neither they nor their rights are threatened[2]. Unless this assurance can be made and is believed, the technology may fail.

Over the past two years, the Center has conducted extensive research to understand public response to its technology, including focus groups and expert interviews in five countries. The reactions can be summarized as 'neutral to negative'. People are willing to accept the technology if, and only if, they can be confident there is appropriate protection from risk and abuse. Privacy rights and health protection are most often cited as areas where reassurance is necessary[3].

This paper discusses how such reassurance could be provided. It is not a proposal or a strategy, but rather is intended to frame, aid and inform constructive discussion. As such, it does not represent an agreed policy of the Auto-ID Center, the Massachusetts Institute of Technology, or any person or organization affiliated with the Auto-ID Center, either explicitly or implicitly. It is a discussion document, and nothing more.

[1] Full information about the Auto-ID Center's Electronic Product Code™ (EPC™) network is available at www.autoidcenter.org

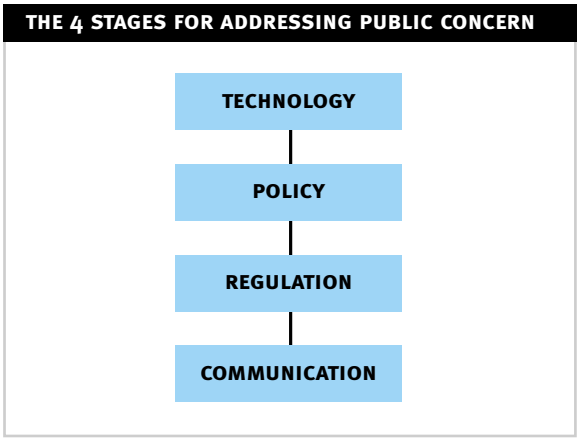
[2] See Brian Cantwell, 'Why Technologies Fail...', MIT-AUTOID-WH016 for more detail.

[3] See Helen Duce, 'Public Policy: Understanding Public Opinion', CAM-AUTOID-EB002 for more details.

2. THE ROLE OF REGULATION

Providing public reassurance about new technology is a 4-step process [Figure 1]. First, the technology must be developed with all due consideration given to protecting the public interest. In the case of the Auto-ID Center, the technology has always been and must continue to be developed with public rights in mind. Second, policy must be proposed to guide how the technology should, and should not, be used. Third, there must be a way to ensure that policy is implemented – this is the role of regulation. Last, there must be public communication about what is and what is not being done.

Figure 1



If there is a critical mass of public concern, these steps will always be taken by somebody. History suggests that if those developing new technology do not develop satisfactory policy and regulation, others will try to do it for them[4]. In extreme cases, the 'policy' will be a sledgehammer: a proposal that a technology must be banned, enforced either by law or by boycott, both of which can be equally devastating. Once significant public concern is evident, regulation of some kind should therefore be regarded as inevitable. The question facing the developers and adopters of a new technology, then, is not 'Would we like regulation?' but rather 'What regulation would we like?'

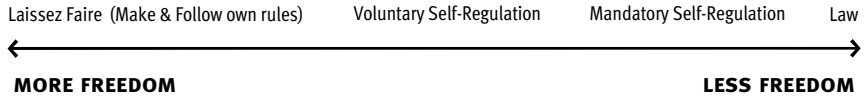
[4] See Brian Cantwell, 'Why Technologies Fail...', MIT-AUTOID-WH016 for more detail.

3. OPTIONS FOR REGULATION

In its broadest sense, 'regulation' covers a wide range of options. At one extreme is pure 'laissez faire' where each entity makes its own policy and regulates itself individually as it chooses. At the other extreme is law: 'policy' made by legislators and enforced by nation states. In between are collective 'self-regulation' approaches, which can either be voluntary, with no penalties for deviation, or mandatory, where deviation can be penalized by the collective (e.g. Trade Body or Consortium) [Figure 2].

Figure 2

OPTIONS FOR REGULATION COVER A RANGE OF POSSIBILITIES



3.1. Evaluating Options for Regulation

Each option is a valid choice in different circumstances.

Laissez Faire works when there is no public concern – it provides great freedom to users or vendors of the new technology, but offers no reassurance to the general public, who are asked to trust that their freedom will not be jeopardized. Given the evidence of public concern we have seen to date, this paper assumes that 'Laissez Faire' is not a sensible option for EPC™ technology.

Collective self-regulation attempts to strike a balance between the desire to remain free of external regulation while reassuring the general public: it can only work if the public believes the process effectively addresses their concerns. It allows stakeholders to directly influence the policy making and implementing process, and is less susceptible to global variations (below). It can also move at a faster pace than legislative processes, which can be an advantage in the fast-moving world of electronics and digital technology. The differences between voluntary and mandatory self-regulation are discussed later.

Laws governing the use of new technology are the most extreme form of regulation. They offer the most reassurance to the general public (in proportion to the public's trust in their government and legislative process), but control is placed in the hands of the state and its political mechanisms. Legislation is a likely outcome if public concern is not addressed sufficiently and quickly via another method. Regulation is most often a 'one-strike and out' game: failure to address public concern can quickly lead to legislation, with potentially more aggressive or punitive laws than may otherwise have been passed.

4. REGULATION AND GLOBALIZATION

Commerce is global but government is national. One effect of legislation on global companies is the imposition of different rules and regulations in different markets. This can add complexity, increase costs and inefficiencies, and make global strategy difficult. It may also force a global business to take a 'lowest common denominator approach' and follow the most restrictive regulations everywhere. In nations where significant legislative powers are held locally (such as the United States) legislation can also mean varying rules within a market. These geographic discrepancies and the complexity they create, coupled with the lack of direct influence over policy, can make legislation a worst-case regulatory scenario for global businesses. Well-executed collective self-regulation, on the other hand, can in theory satisfy the public around the world and make legislation unnecessary – or at least minimal – everywhere.

5. SELF-REGULATION: MANDATORY VERSUS VOLUNTARY

[5] To quote one Board of Overseers member: 'I don't like mandatory anything'

The option for mandatory self-regulation – that is, 'follow the rules or there will be penalties' – exists in any area where there are technical or legal means to enforce policy. This is the case with EPC™ – there are a number of remedies available to give 'teeth' to mandatory self-regulation. The most extreme of these is deregistration from the Global Root Object Name Server, which could render a company's EPC™ useless beyond its own walls. Other remedies, for example based on license conditions, are also feasible. Either mandatory or voluntary self-regulation could therefore be applied to the EPC™ Network. The word 'mandatory' can repel some people automatically [5], but there is nothing more mandatory than the law, and mandatory self-regulation has advantages over legislation. Specifically, self-regulation can be the same globally, and businesses can exercise far more control over the policy development process. Mandatory self-regulation requires work and collective willpower. There needs to be a process for investigating whether policy is being followed, and a readiness to address non-compliance. This is not as easy as a laissez-faire or voluntary approach.

Voluntary self-regulation has the advantage of reserving the freedom of each individual company, but may instill less public confidence. It also runs an obvious risk: one 'bad apple' that ignores the regulations and misuses the technology either deliberately or in ignorance may precipitate legislation for everybody and, even worse, do harm to somebody. This possibility naturally increases with every new user and every new country that adopts the technology.

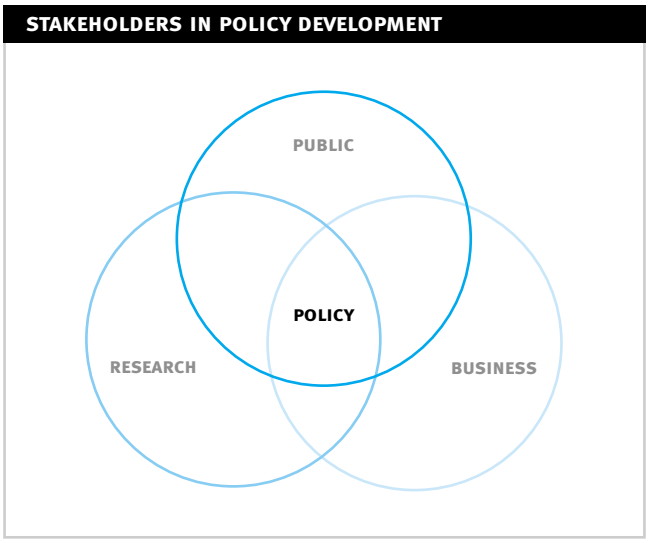
6. FORMULATION OF POLICY

[6] The following is an illustrative proposal, for discussion purposes only.

How policy is formulated should be a central question in any discussion of regulation. One advantage of self-regulation is that it is easier for business users to influence policy in a self-regulatory environment. It is therefore reasonable to consider how policy might be formulated if self-regulation for use of EPC™ were to be adopted [6].

The best policy development processes considers the interests of all stakeholders with sincerity, honesty and balance, and are based on good information. In the case of EPC™ there are three groups of stakeholders, each of whom should be represented equally and independently. These are the public, the Business community (divided between vendors and users) and the Research community. [Figure 3]

Figure 3



Each group has an essential role to play in policy development.

The public is the ultimate customer for regulation, the main purpose of which is to protect the public interest. The public would be represented in the policy development process by the Auto-ID Center's independent Policy Advisory Council, who could also conduct outreach and dialogue with special interest groups, consumer advocates and other public representatives [Figure 4]. Details of current Council members are given in an appendix to this document.

Figure 4: Inaugural meeting of the Auto-ID Center's independent Policy Advisory Council, Massachusetts Institute of Technology, November 6, 2002

Researchers have a vital role to play in the policy development process. Unencumbered by commercial interests, they can offer objective perspective on what is possible technically, both in terms of abuse of the system and also means of protection from abuse. They can anticipate future considerations, and can also use what they learn in the policy development process to continuously improve the security of the technology in the public interest.

Business representatives from both the vendor and user community must be involved in policy development – indeed, the opportunity for them to influence policy so directly is one of the main advantages of self-regulation over legislation. Why must business be involved? One reason is that business users and their vendors have to be able implement any policy that is proposed. A policy that cannot be implemented – for example because it is impractical or not economical – has no value.

Small groups representing each of these three stakeholders should meet regularly to continually refine policy via a consensus-driven process. These small groups could, of course, be delegates or subsets of larger caucuses.

7. CONCLUSIONS

This is a discussion document. Its purpose is not to recommend a course of action, but rather to frame debate. That said, some conclusions and comments about regulation of the EPC™ network appear to be self-evident:

- The public needs to be reassured about the use of EPC™ technology. It is not enough to create policy. There must also be a process for implementing policy. A 'Laissez Faire' approach is unlikely to be acceptable. Some form of regulation therefore seems inevitable.

- From a business perspective, self-regulation has advantages over legislation. It is better suited to a global trading environment, and allows for more direct business influence over policy and its implementation. It may also be preferable for some legislators, as it can move faster to keep up with changing technology.

- Mandatory self-regulation of the EPC™ network is feasible, if desired.

- Any attempt to self-regulate must be a sincere attempt to protect the public interest, or it risks backlash and potentially severe legislative consequences. Putting business freedom before public freedom is a mistake.

Further discussion among stakeholders is required before any decisions can be taken, but it seems clear that decisions must be made very soon. As the Auto-ID Center's Field Test and other EPC™ pilots progress during 2003, and press coverage of this activity increases, the public will need the reassurance of an acceptable usage policy, and an acceptable means of implementing it, and soon. If the Auto-ID Center community does not do this, others will rush to the task.

APPENDIX

The Auto-ID Center's Independent Policy Advisory Council

Elliot E. Maxwell
Chairman

Elliot E. Maxwell is a Fellow of the Center for the Study of American Government at Johns Hopkins University, Distinguished Research Fellow at the eBusiness Research Center of the Pennsylvania State University, and chair of the International Policy Advisory Council of MIT's Auto-ID Center, www.autoidcenter.org

From 1998 until 2001, Maxwell served as Special Advisor for the Digital Economy to U.S. Secretary of Commerce William Daley and U.S. Secretary of Commerce Norm Mineta. In this position he was the principal advisor to the Secretary on the Internet and E-commerce. He coordinated the Commerce Department's efforts to establish a legal framework for electronic commerce, ensure privacy, protect intellectual property, increase Internet security, encourage broadband deployment, expand Internet participation, and analyze the impact of electronic commerce on all aspects of the economy. He was deeply involved in the development of E-government activities and was a founding member of the Federal Interagency Working Group on Electronic Commerce.

After leaving the government he was Senior Fellow for the Digital Economy and Director of the Internet policy Project for the Aspen Institute's Communications and Society Program. The Communications and Society Program focuses on the impact of communications and information technologies on democratic institutions, the economy, individual behavior, and community life.

Maxwell graduated from Brown University and Yale University Law School. He has written and spoken widely on issues involving the Internet, electronic commerce, telecommunications, and technology policy. His most recent work, "Rethinking Boundaries in Cyberspace", written with Erez Kalir, has been published by the Aspen Institute and is available at http://www.aspeninstitute.org/c&s/pdfs/rethinkcyberspace.pdf

Alex Allan

Main areas of expertise
- **E-commerce, internet, telecommunications etc**: worked as British Government's first e-envoy, promoting and co-ordinating policy on e-commerce and on getting services online.
- **Formulation and implementation of Government policy**: spent over 5 years as the Principal Private Secretary to the Prime Minister in the UK, involved in almost every aspect of Government policy and administration.
- **International and domestic financial issues**: much of career on international issues in Treasury. Then acted as the UK's "Sherpa" for G7 Economic Summits. Also experience in Treasury on tax, spending and domestic financial regulation.
- **International relations**: served as British High Commissioner to Australia from 1997–99.

Career
2001
Working for a PhD in the Faculty of Business & Public Management at Edith Cowan University, Western Australia. Member of the Premier's Science Council in WA. Member of the International Advisory Panel to the South Australian Government for their IE2002 program.

1999–2000
E-envoy for the British Government. Responsible for co-ordinating policy across Government on e-commerce (legal framework, international issues, telecommunications regulation, education and training, access initiatives etc), and for overall policy on getting Government services online. See http://www.e-envoy.gov.uk for further information and most recent reports on achievements.

1997–1999
British High Commissioner to Australia. Responsible for British trade policy, diplomatic and consular work across Australia.

1992–1997
Principal Private Secretary to the Prime Minister (John Major to April 1997 and Tony Blair to Aug 1997). Responsible for all the work of the Prime Minister's office, overseeing advice and briefing on both policy and communications. Appointed G7 "sherpa" for Naples, Halifax, Lyons and Denver Summits.

1990–1992
Under Secretary, General Expenditure Policy, HM Treasury. Responsible for overall planning of public expenditure policy and programs.

1989–1990
Under Secretary, International Finance, HM Treasury. Responsible for policy on IMF and World Bank programs, as well as analysis and briefing on world economic trends. UK negotiator for agreement setting up European Bank for Reconstruction and Development.

1986–1989
Principal Private Secretary to the Chancellor of the Exchequer (Nigel Lawson). Oversaw all briefing and advice, covering international finance, economic and taxation policy.

1985–1986
Principal, Reform of Local Government Finance, HM Treasury.

1983–1984
Freelance computer consultant in Sydney (1983) and Perth (1984). In Sydney, primarily worked on projects developing accounting software. In Perth, worked on yachting applications.

1976–1982
Various job in HM Treasury (exchange rate policy, balance of payments, industrial policy etc).

1973–1976
Administration Trainee, HM Customs and Excise. Worked on introduction of VAT (GST).

Education

1972–1973
MSc in Statistics, University College, London

1969–1972
BA(Hons) Mathematics, Clare College, Cambridge

1964–1969
Harrow School

Dr. Herbert Burkert

Current Positions/Activities

- President, Research Center for Information Law, University of St. Gallen, Switzerland.
- Chairman, Legal Advisory Board to The European Commission's DG "Information Society".
- International Fellow, Information Society Project, Yale Law School, New Haven, USA.
- Member of the Cologne Bar.
- Visiting Professor at the University of Namur, Center for Computer and Law (CRID), Namur, Belgium.
- Law, Political Science and History at the Universities of Cologne and Dublin; Research Fellow at the University of Regensburg, Germany; PhD University of Frankfurt am Main ("summa cum laude"); Habilitation (equivalent to a second PhD) University of St. Gallen.

Areas of Work

- Information and Communication Law, History and Public Policy Issues of Media and Law; International Privacy and Freedom of Information Issues; Information & Knowledge Policies.

Editorial Boards

- Multimedia und Recht, Datenschutz und Datensicherung (Germany); Electronic Commerce & Law (USA); Journal of Law and Information Science (Australia); Media Lex (Switzerland); Revue de Droit de l'informatique et des Télécoms (France); Revue Ubiquité (Belgium).

Simson L. Garfinkel

Simson L. Garfinkel is a researcher in the field of computer security and commentator on information technology. As a researcher, Garfinkel is currently a graduate student at the Laboratory for Computer Science at the Massachusetts Institute of Technology, where he is working on his doctorate. Prior to joining LCS, Garfinkel founded Sandstorm Enterprises, a computer security firm that develops offensive information warfare tools used by businesses and governments to audit their systems.

Garfinkel founded Vineyard.NET, the Internet Service Provider (ISP) for Martha's Vineyard, in 1995. In 2000 he successfully negotiated the sale of Vineyard.NET to Broadband2Wireless (BB2W), a venture-funded broadband wireless ISP. When BB2W failed, Garfinkel negotiated the repurchase of Vineyard.NET from BB2W's bankruptcy court.

Besides his activities as a computer scientist and entrepreneur, Garfinkel has had an active career as popularizer of technology. After receiving his masters degree from Columbia University in 1988, Garfinkel spent 14 years writing for some of the nation's leading publications, including **The Boston Globe**, **The San Jose Mercury News, The Christian Science Monitor**, and **Technology Review Magazine**, in which he now publishes a regular column. He was one of the founding contributors of Wired Magazine, and still writes for Wired on an occasional basis. Garfinkel's popular articles have appeared in more than 50 publications including **ComputerWorld, Forbes, The Nation, The New York Times, Omni and Discover.**

Garfinkel is the author or co-author of twelve books on computing, published by O'Reilly and Associates, MIT Press, Springer-Verlag, and IDG Books. He is perhaps best known for his book **Database Nation: The Death of Privacy in the 21st Century**. Consumer advocate Ralph Nader called this book "A graphic and blistering indictment" of the techniques used by businesses to invade our privacy and our lives. Garfinkel's most successful book, **Practical UNIX and Internet Security**, has sold more than 125,000 copies since the first edition was published in 1991.

Garfinkel holds three degrees from the Massachusetts Institute of Technology and a masters of Science degree from Columbia University. He is a member of the Association for Computing Machinery (ACM), Computer Professionals for Social Responsibility (CPSR), and has a certification in computer security (CISSP) from International Information Systems Security Certifications Consortium. He has been a fellow at the **Berkman Center for Internet Law and Society**, and remains a Berkman affiliate. He is also an FAA licensed pilot, although he doesn't get to fly much these days.

Garfinkel's CV is located on the Internet at http://www.simson.net/cv. Garfinkel lives in Belmont with his wife and three children.

Dale N. Hatfield

Dale N. Hatfield is an Annenberg Senior Fellow and founder, former President, and current Chief Executive Officer of Hatfield Associates, Inc., a consulting firm specializing in engineering, economic, and policy studies in the telecommunications field. Currently Adjunct Professor at the University of Colorado, Hatfield was founding Director of the Telecommunications Division at the University of Denver. He is a former Deputy Assistant Secretary of Commerce for Communications and Information; Deputy Administrator of the National Telecommunications and Information Administration, U.S. Department of Commerce; and Chief of the Office of Plans and Policy at the Federal Communications Commission. Hatfield frequently speaks before industry groups and testifies before Congress. He holds a B.S.E.E. from Case Institute of Technology and an M.S. in Industrial Management from Purdue University.

Takato Natsui

Takato Natsui is a professor of Legal Informatics at Meiji University Law Faculty and Meiji University Graduate School of Law, Tokyo, Japan. He obtained his Bachelor of Economics degree at Yamagata University in 1978. He was an assistant judge at Nagoya district court in 1983, an assistant judge at Morioka district court in 1985, an assistant judge at Chiba district court in 1988, a director at Sendai district court Kesen-numa branch in 1991, an instructor of Civil Laws at Court Clark Instruction Institute of Japanese Supreme Court in 1993, a chief instructor of Civil Laws at Court Clark Instruction Institute of Japanese Supreme Court in 1994, a judge at Tokyo district court in 1995, and he became a professor at Meiji University in 1996. He is also an attorney at law registered at the Tokyo Bar Association in 1997.

Professor Natsui's major areas of concern are legal informatics, legal philosophy and Cyberlaw, especially the analysis of legal information, legal database development, cyber crime, electronic commerce, electronic signature law, intellectual property rights relating to digital contents, and legal procedures using the Internet.

He has been a representative of the Cyberlaw Study Group Japan and the Legal Informatics Study Group Japan. In 2002, these study groups were combined and reconstructed as a new academic association called the Information Network Law Association Japan of which he is a vice-chair.

Professor Natsui was a board member of the Japanese Association of Law and Computers and is a member of the Cyber Criminal Legislation Study Group at the Ministry of Economy, Trade and Industry (METI).

He has also been a project leader of SHIP project (Social, Human and Information Platform project) that is a progressive study project for developing XML based legal database systems funded by Meiji University and the Japanese government. His latest English publication (editor) is "SHIP Project Review 2001 (2001)".

Designed and produced by Foxner. www.foxner.com