Economic Aspects of Biometric Technologies[1]

By Jonathan Cave

3.2.1 Introduction

Economic transactions require *trust*. Secure provision of identity can build needed trust by fixing liability and facilitating legal recourse. In addition, identifying oneself can signal goodwill. *Personalising* data by tying them to identities provides convenient summaries that improve market matching of tailor-made demand and supply. More generally, identity *indexes* transaction history or other data.

Identity also serves as a *capital* asset (e.g. credit ratings) - formed through investment and subject to depreciation. Ownership of identity capital may be split or diffused (e.g. credit rating agencies with different accounts and amounts of information). This increases the need to attach the data to the person seeking credit.

These functions of identity were known in economics for a long time, but identification was not really an economic issue – face-to-face or closed-system transactions lacked significant misidentification risk and identity fixation in remote transactions or open systems tended to be a legal matter. The value of identity was also approached obliquely – primarily via analysis of reputations. Recent changes in technology and practice call for fresh economic perspectives. Increasingly 'virtual' transactions - where parties may never be able directly to verify each other's identity - have increased the value of identity and made identity theft a more pressing concern. Technical 'solutions' offer identification of differing strengths; their interoperability affects the compartmentalisation of economic identity and its externalities.

The impact of biometrics on economic outcomes will be discussed: optimal and actual identity, the emergence of standards, and costs and benefits. A second section surveys the present state and likely evolution of market demand and supply. Finally, the issues which policy makers need to address as well as the means to address these issues are explored.

3.2.2 Economic aspects

3.2.2.1 Optimal identity

In cash transactions parties need not be identified; it is only necessary to verify the right to exchange goods and services for money. However, uncertain or contingent transactions may need more. Buyers may need to prove creditworthiness or certify how purchases will be used, sellers may need to establish provenance or certify quality, origin, etc. via retrospective (e.g. professional qualification) or prospective (e.g. seller warranty) identity. Sometimes it suffices to prove membership of a

[1] Authored by Jonathan Cave, Senior Lecturer at the Department of Economics, University of Warwick, Coventry, UK, and research leader with RAND Europe, Cambridge, UK, this section is a brief summary of the report on "Biometrics: economic issues and implications", to be found online at www.jrc.es

specified class (adults, physicians); other cases require identification of specific individuals or their legal representatives.

Even if biometrics provides more certain identification it is not necessarily cost-effective or 'optimal' because its additional costs may exceed the benefits of increased certainty of identification. The quality of a particular implementation may be too high for at least one party. Some – regardless of monetary cost – may be too strong for the purpose for which they are employed due to privacy concerns or legal restraints on information collection. Permissible accuracy may be limited – for example, it is essential to establish that voters are eligible and have not already voted, but equally essential not to identify them further. Unless the means and degree of biometric identification are included in negotiations there is no reason to expect optimal identification; there may be too much or too little identification or use of secure channels.

Generalised use of one or several large and widely-used "strong identification" systems provides an enormous installed base to cover e.g. security and RTD costs and scope for data mining to detect fraud, thus lowering costs and increasing security. It also limits identity compartmentalisation to control risks. However, even apart from increased data protection concerns, its very strength makes errors harder to correct. 'Hardening' outer boundaries may reduce overall security if internal precautions are relaxed. Identity theft may be less frequent but more severe and identity theft may give way to outright 'denial of identity service' attacks.

Furthermore, to the extent that biometrics provide cheaper, stronger and/or faster identification, they 'tilt the playing field' against those who cannot or will not participate. If the vast majority migrate to a biometric solution, alternative channels may disappear, excluding or imposing costs on the minority. Those with privacy concerns may be unable freely to opt out without losing access to goods, services or societal interactions to which they are entitled –harming those on the 'inside' as well. Due to network effects, any system whose benefits depend on user interactions will be damaged by changes that raise barriers among users.

3.2.2.2 The emergence of standards

Biometric implementations have technical and dynamic efficiency effects common to network technologies. Identity is *complementary* to economic transactions, so equilibria may be unstable or non-existent. Economies of scale and interoperability favour winner-takes-all ("tipping") equilibria. This works by three channels:

- Market adoption depends on *expectations* – a technology expected to become a standard is likely to do so.
- Competitive forces are likely to produce a single (or unified) standard approach, especially with greater interconnection among sectors and participants, so early leads are difficult to overcome.
- "Sunk costs" of adopting standards can strand those making the 'wrong' choice with obsolete investments and reduced benefits. This risk makes firms wait to adopt, particularly where value depends on availability of interoperating and complementary database, communication, sensing, payment, etc. systems. This in turn inhibits investment in developing such complements, and partially accounts for private sector reluctance to adopt biometrics despite falling direct costs.

This tendency to "tipping" is reinforced by pressures for compromise solutions. If interoperability were irrelevant, it would be possible to match each application to that

biometric offering the best combination of costs, accuracy, etc. But even closed identity management systems need to interoperate[2] and multiple identity systems impose substantial burdens. Even when 'optimal' biometric solutions differ by application area, there are strong pressures to adopt imperfect compromise solutions.

Another mechanism which might undamaged competition could be strategic use of intellectual property rights (IPR). A firm holding key patents need fear no competition; if it chooses to allow competitors to licence its technology, it can do even better, encouraging entry of efficient rivals and extracting further rents from their innovations. Ultimately, such strategies are self-defeating; they encourage bypass competition and antitrust action, keep prices high and limit market growth and prevent the 'medicine of competition' from driving costs further down. But, as recent iris scan algorithm patenting disputes show, such self-defeating tactics still persist[3]. Further ramifications include patent 'thickets' and 'clusters' to deter innovative rivals.

There are two alternatives to the emergence of *de facto* (proprietary) standards as a result of "tipping", IPR or accident: voluntary industry agreements (typically open); and mandated national or international standards. Open standards are more likely to solve the coordination problem and enhance competition by lowering entry barriers and stimulating innovation of complementary products. However, they may take longer to achieve and can mask collusion. Mandated standards can be established quickly – perhaps too quickly if they are based on uncertain assessments (e.g. ISDN) or forestall price and quality competition. Regulators may be captured by better-informed industry players, amplifying the anticompetitive effect of proprietary standards.

3.2.2.3 Costs and benefits

Decisions about biometrics rest on estimates of costs and benefits, relative to alternative means of identification, which offer both advantages (ease of issue or revocation, no problem of template aging, low entry barriers) and disadvantages (vulnerability, 'hidden cost' of lost or multiple passwords). Early adopters have high direct costs, but enjoy increased chances of 'winning' the standardisation race, incentives for further development and IPR and 'learning curve' reduction of future costs, including indirect costs[4].

On the benefit side, available data tend to fall into three categories:

1. Costs of problems biometrics should solve.

   Annual UK costs for identity theft[5] are estimated at €1.95 Billion (10% of all fraud, and growing). In the US, where it quadruples annually, identity theft affected 28 million citizens and cost €55.5 Billion in 2003. However, the degree to which biometrics reduces theft and the possible displacement of fraud remain uncertain.

---

[2] With other biometrics in combined systems and with data, payment, CRM, etc. in integrated applications.

[3] The main patent is due to expire shortly. The patent holder guarded its rights jealously, launching attacks against actual or potential rivals even in the waning days of the patent.

[4] For instance, automated identity management can produce personnel savings – or raise the cost-effectiveness of skilled personnel. Conversely, there may be increased demand for skilled staff to enrol participants or decreased capability to perform other tasks at point of verification.

[5] For US data, see e.g. http://www.consumer.gov/idtheft/stats.html. For the Cabinet Office report (2002), see http://www.homeoffice.gov.uk/docs/id_fraud-report.pdf.

2. Cost savings from immediate deployment.

   Such data are often proprietary or commercial. They should be presented as lifetime cost of ownership and adjusted for changes in financial, physical, IT and human capital and impacts on internal processes.

3. Estimates of willingness-to-pay

   These estimates provide a lower bound on consumer surplus from biometrics. Better functionality is accompanied by falling costs: the two effects offset in terms of price but should be added to estimate welfare gains. Biometrics also let risk-averse consumers save on costly hedging or insurance or make use of more secure or competitive channels.

3.2.3 The biometrics market

3.2.3.1 Demand

In the recent past, three applications have constituted the bulk of the biometrics demand. Firstly, physical access control has been the dominant application since the advent of biometrics, but is rapidly being supplanted by IT applications. It had 42% of the biometrics market in 2000, was dwindling but revived strongly since 9/11. Here the dominant trend is expansion to monitor time, attendance or physical location. IT applications had the second-largest share of the market (25% in 2000), growing with biometrics' inclusion in laptops, the development of specific interface standards and biometric implementations in converged computing/communications equipment. The third largest area for biometrics was financial services (15% in 2000), which is likely to grow due to changes in fraud types, financial identity management and banking itself.

However, the demand for biometrics is rapidly shifting, due to new implementations. Government and other public sector applications will be leading the sector in volume, new technology adoption, project scale and prominence. After 11 September 2001 transport and immigration (biometric passports) have become key issues, with an emphasis on international interoperability. The public sector is also a leading client in health, where biometrics is increasingly used to prove entitlement and link patients to electronic health records.

Other sectors likely to emerge as significant parts of the market are retail and other payments - already being trialled in wide range of applications, telecommunications services - integrated with other services and linked to individual data, and transport - including private transport.

3.2.3.2 Supply

The biometrics sector follows the 'experience curve:' a few leading firms, many subsequent entrants and consolidation to a few survivors. The shakeout is well underway; despite strong demand growth, mergers and bankruptcies dominate recent market reports. The cycle is more advanced in fingerprint, while newer technologies (iris) still have many small firms pursuing diverse approaches (albeit with tight control of key patents). Concentration is high even during expansion, leading to persistence of dominant firms with specific national and/or sectoral attachments and possible distortion of biometric development.

The tendency to concentration is reinforced by specific factors. Firstly, as eventual uses of the technologies are unclear, fixed testing costs are fairly high, which raises

entry barriers. Secondly, early public or private customers seek 'assurance,' which favours incumbents and firms with a large installed base. The key role currently played by very large public procurements can generate an enormous installed user base, which encourages subsequent clients and suppliers of complements to standardise on the incumbent firm/approach. Thirdly, the threat to competition is enhanced by the 'layered' structure – hardware, middleware, application, all of which must work with each other. Market power in one layer can extend to others.

3.2.3.3 State of the market

The industry began and is thriving in the US, but Europe's share is growing rapidly, particularly in banking. Recent European government initiatives will boost demand even more. Available data suggest consistent dominance by fingerprint, with hand geometry and voice recognition dwindling and iris growing.

Supporting these data are overall growth and the growing non-US market (where hand recognition is rarely used). Strong revenue growth in fingerprint is likely to continue as cheaper scanners are bundled with computers. Facial recognition and iris also show strong growth (Figure 1).

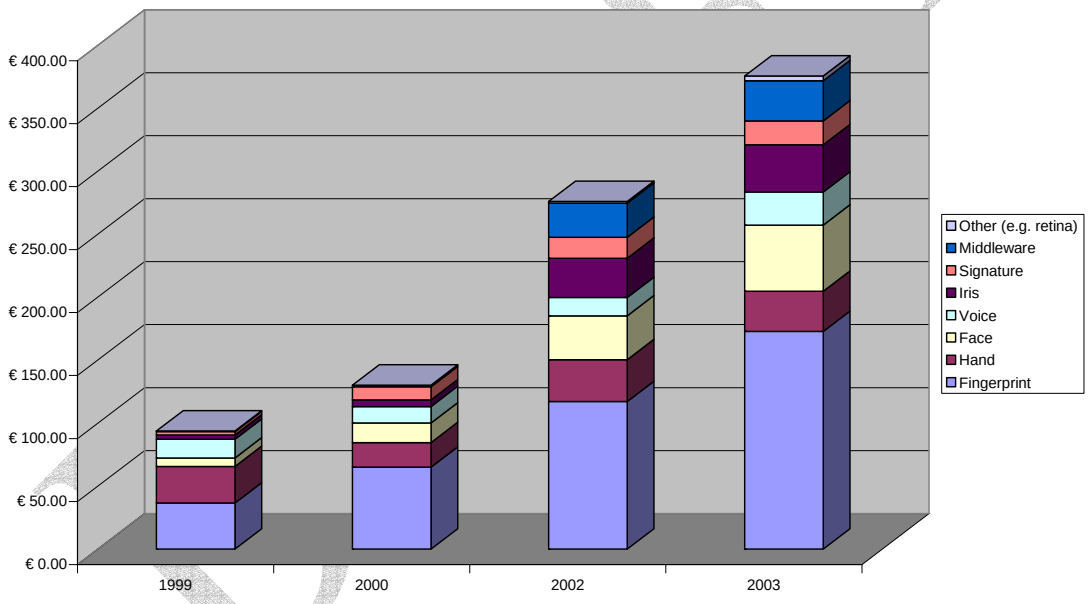

Figure 1: Revenues by technology

Over time, hardware will become cheaper, interoperable and commoditised. Algorithms will remain proprietary and distinctive and continue to improve, so IPR will remain profitable. Middleware, which mediates functionality and interoperability, is likely to be convergent, less profitable and ultimately provided by open-source and/or compatible free software.

Application service providers will dominate the growth phase – initially providing solutions but ultimately supporting users and 'intermediary' layers, possibly before acquisition by integrators. Value-added resellers and original equipment manufacturers provide important transitional competition, but the market is likely ultimately to belong to specialised security or diversified ICT integrators. Relationships are likely to be strategic and/or collusive partnerships. Ultimately,

biometrics may be wholly subsumed by technology (e.g. PCs), integrated ICT and/or security markets.

3.2.4 Policy

Six major issues which might require action by policy makers emerge from the above analysis.. In a second step, we will present the levers which policy makers have at their disposal to address these issues.

3.2.4.1 Issues

The first is possible *market failure* – competition may be undermined by 'tipping' or capture – of a single market layer or a set of connected segments. This applies to biometrics *per se* and broader IT, transportation, health informatics, etc. market segments, in many of which strong network, interoperability and complementarity effects can lead to some dominance. The consequences are those usual to competitive failure; allocational inefficiency, retarded or distorted RTD and associated spill-over effects on employment, competitiveness, etc.

A second, somewhat narrower concern is the *development and competitiveness* of biometrics and the 'identity industry'. Biometrics shares many characteristics with other high-tech industries (risk, possible slow take-up, limited capital access, threatened obsolescence, high-tech skill dependence, critical importance to other rapidly-growing sectors), but stands out because of its importance to security, eGovernment and other public objectives.

The third concern is the tension between *standards* 'lock-in'[6] and diversity. Market competition on its own may fail to produce timely and appropriate levels of standardisation or may get 'stuck' in an inferior standard.

Fourthly, *intellectual property rights* (IPR) are obviously important to the competitive health of the market, but pose particular problems relating to interoperability and network effects. Compatibility requirements may reward IPR holders with market power even without beneficial innovation – especially when customers value stability, 'assurance' and compatibility above other characteristics. The first product to be adopted may well become the *de facto* industry standard. On the other hand, IPR may encourage beneficial 'bypass' innovation.

A fifth point is that biometrics is a key element of government *security* policy. Yet governments have poor records in managing large IT procurements, and political sensitivities combined with rapid technology development and the importance of international interoperability make value for money even harder to ensure. For instance, it is not obvious who (if anyone) 'owns' liability for flaws in a technology or its implementation. On the basis of empirical evidence, open-source systems seem to be at least as secure as proprietary systems and sometimes much more secure[7].

Finally, the use of one's identity itself is changing from a 'private good' belonging to the individual and useful in a limited range of close interactions to a form of social capital used in a vast range of poorly-observed and uncontrolled interactions and based on data scattered throughout many networks. Difficulties in preventing access to one's identity and its possible abuse in ways that are not immediately obvious

[6] Arthur (1983), David (1985).
[7] Compulsory licensing provides a limited 'third way' but is costly and legally complex to operate.

makes ‘identity’ a *public good* – not least because protection of individual rights and freedoms may require public provision of strong identity.

3.2.4.2 Policy levers

These issues can be addressed by several policy levers. The first is *procurement policy*. Large government contracts are often the first major demand component, underwrite private financing and create industry leaders in a short space of time. Thus they drive new technologies. The advent of mass-market biometrics coincides with security, eGovernment and eParticipation initiatives. However, the public sector’s ‘launching customer’ role is extremely difficult; it requires appropriate specification, smart contracting and active partnerships with suppliers in the face of untested technology. Because biometrics is intimately connected with sensitive policy areas it may challenge the two pillars of European public procurement: equal treatment and transparency. Tools include ‘pre-competitive engagement’ multiple-sourcing, design competitions, IPR options in contracts, open standards requirements and insistence on open and transparent supply chain management. Interoperability generally makes it impossible to divide procurement among many firms in advance of open standards, but procurement can be structured to leave even ‘losers’ with valuable IPR and to provide opportunities for integrators, licensees, etc. to participate in future development.

A second policy lever is *standardisation policy* – there is a potential role for mandated open standards with protection for ‘equivalent’ alternatives or for incorporation of open standards requirements in procurement, licensing and other policy decisions.

As a third lever, *competition policy* must take account of both tipping tendencies and the need for innovation. In general, incompatibility makes product innovation ‘too fast.’ Another danger is *foreclosure* e.g. when an integrated provider deliberately makes its equipment incompatible with rival offerings or when the holder of a key patent effectively controls all those who use it. Competition policy can act via merger and access pricing regulation. The treatment of industry standards consortia is also important; they might manipulate standards, exchange cost information or refuse to licence to ‘outsiders’.

The fourth policy domain are *intellectual property rights* (*IPR)*. There is obvious scope to use mutual recognition and compulsory licensing to control adverse effects or private IPR. A more radical alternative would be a public goods route (e.g. General Public Licence) supporting an open source RTD policy, where access to research results is open, usage rights are granted freely and even derivative innovations may be bound to the public domain. Economic returns may be sought in selling related goods and services or in selling enhanced versions.

The following Table summarises the interaction between issues and levers.

		Policy domains			
		Procurement	Standards	Competition	IPR
Issues	Market failure, sector health	✓		✔	✓
	Standards	✓	✔		✓
	IPR	✓	✓	✓	✔
	Security	✓			
	Public identity	✓			