International Review of Law, Computers & Technology
Vol. 24, No. 2, July 2010, 153–162

Protecting privacy in automated transaction systems: A legal and technological perspective in the European Union

Faye Fangfei Wang[a]* and Nathan Griffiths[b]

[a]*Bournemouth University, Bournemouth, UK;* [b]*University of Warwick, Coventry, UK*

In the past, spies could enter one's residence, organisations or companies and collect valuable information such as personal sensitive data, trade secrets or transaction records. Nowadays, the open architecture of the Internet has generated an environment in which there are more opportunities to quickly and easily obtain data than there used to be, as a variety of sensitive information can be captured on the Internet without a physical presence in the location where the data is situated. Privacy rights have consequently become more vulnerable to attack. This paper will discuss the current legal framework of ePrivacy protection in the European Union (EU), examine the state-of-the-art technologies for service-oriented computing, evaluate practical obstacles and propose possible solutions to establish trust in privacy management.

Keywords: privacy; data protection; service-oriented computing

1. Introduction: data and eprivacy protection

Privacy, as a fundamental human right, has been protected under basic laws in different countries or conventions at the international level since the 1950s. From a boom of electronic commercial transactions in 2000, data protection stemming from international computer networks has been challenged owing to technical and legislative obstacles. Data protection constraints on the Internet are preventing online users' privacy rights from being fully protected. For example, in B2C (business-to-consumer) transactions, an online retailer might have a database of information about its consumers' personal details and their history of transactions in automated selling systems. In B2B (business-to-business) transactions, automated transaction systems create the possibility of automated composition, automatic negotiation, i.e. service-oriented computing (SOC) generates automatic management of quality of service in B2B business, while automated computing (AC) allows high frequency trading known as super fast automated trading. All sensitive information of the trading parties (i.e. providers and customers) can be captured by the system in a split second. It is reported that one computer system of automated trading can currently be sized to handle about 400,000 transactions a second. With the advent of computing power, information travels more freely with very little need to have human intervention. The Internet makes it possible for individuals to react and trade in real time with each other from anywhere on the globe. It also reduces the cost of transactions, for example,

*Corresponding author. Email: fwang@bournemouth.ac.uk

ISSN 1360-0869 print/ISSN 1364-6885 online

DOI: 10.1080/13600861003748243
http://www.informaworld.com

in stock markets a trade can be executed in less than a second, probably for just a few dollars. The logic of profit margin via automated trading is as follows:

> As I entered the stock at 35 cents, in an automated way, someone has come out and sold at 34 cents stock, 33 cents stock ahead of my offer. They are trying to sell stock ahead of me to take advantage of getting higher prices before I start selling it. Their hope is that they just sold 800 shares at 33 and 34 cents and the stock is going to go down and they'll be able to buy those shares back cheaper, and that's how they're hoping to make money.[1]

The process is simple, since it is essentially a matching engine. When a willing buyer meets a willing seller at an agreed price, the transaction is executed straightaway. Or in the case of a service agreement, when the standard or condition meets the service requirements, the agreement is automatically concluded. The simplicity of the automated transaction system facilitates the efficiency of commercial transactions. Business partners' bank details and business strategies are also kept on the automated computer servers. However, it also increases the risk of insecurity. For example, what will happen if a third party steals the information or if the database owner sells the information to the third party?

In order to build users' trust and confidence, many online trading or service companies, have posted self-regulations on their webpages. However, it is doubtful how many users have actually read the privacy statements in the small print or via a clicked link before using a service or placing an order. It is also questioned whether companies do keep their promises and comply with their self-regulated privacy policies. If not, what are the remedies?

In response to the necessity of e-privacy legislation, countries have made efforts to regulate the rules of e-privacy in order to facilitate economic growth, cooperation, trade and investment. This paper will discuss the current legal framework of ePrivacy protection in the European Union (EU), examine the state-of-the-art technologies for service-oriented computing, evaluate practical obstacles and propose possible solution to establish trust in private management.

2. ePrivacy legal framework of the EU

Data protection is to protect the rights of data ownership and balance the benefits between the protection of data ownership and the permission of data free-flow, while privacy protection is to protect fundamental human rights. In the EU, according to Article 1 of the EC Directive on Data Protection (1995),[2] the EC Directive on Data Protection is not only to protect personal data but also individual privacy rights. The EC ePrivacy Directive[3] supplements the EC Directive on Data Protection. It reflects on Recital 6, 12 and Article 1 of the EC ePrivacy Directive. For example, Recital 6 of the EC ePrivacy Directive states that

> the Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal *data* and *privacy.*

Recital 12 further clarifies that it is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. It also

> harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community

as stated in Article 1(1) of the EC ePrivacy Directive.

Although the EC ePrivacy Directive complements the EC Directive on Data Protection providing privacy protection particularly in the electronic communication sector, some provisions of the EC ePrivacy Directive are narrow and non-specific. For example, Article 4 ('Security') and Article 6 ('Traffic Data') need to be amended regulating the liability of data infringement. On 13 November 2007, the European Commission adopted a Proposal for amending the EC ePrivacy Directive. In response to the proposal, the European Data Protection Supervisor (EDPS) released his second Opinion on ePrivacy Directive review and security breach in January 2009.[4] The EDPS welcomes the adoption of a security breach notification system as it will encourage companies to improve data security and enhance the accountability of the personal data.[5] That is, network operators and Internet service providers (ISPs) should notify security breaches to the national regulatory authorities (NRAs) and also their customers. However, it is argued that the communication is unclear in terms of its scope of the organisations that are subject to breach notification as it seems to only refer to IT companies in the EU, whereas most state legislation in the USA applies horizontally to all organisations that process certain types of information.[6]

The substantial issue of the liability of infringement of privacy rights shall be governed by national laws. As stated in Recital 55 and Article 23 of the EC Directive on Data Protection, any person who has suffered damage is entitled to receive compensation from the controller, as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive. Article 15(2) of the EC ePrivacy Directive also provides that the provisions of judicial remedies, liability and sanctions of the EC Directive on Data Protection shall apply with regard to national provisions adopted pursuant to this Directive. An example can be given by a leading case in the UK that hit the headlines in 2008. In the UK case of *Applause Store Productions Ltd and Firsht v. Grant Raphael* (hereafter 'Facebook' case [2008] EWHC 1781 (QB)), the claimant Mathew Firsht, the owner of Applause Store Productions, was successful in an action alleging libel and misuse of private information. It is a lawsuit against the claimant's former friend, Grant Raphael, who created a false profile for Mathew Firsht on Facebook without his consent. The defendant published the claimant's sensitive personal information on Facebook and created a link called 'Has Mathew Firsht lied to you?' that defamed Firsht's business in providing audiences for a popular television program. The Judge Richard Parkes QC ruled that the claimant, Mathew Firsht, was awarded £2000 as damages compensation for his hurt feelings and distress caused by the defendant's misuse of private information, along with the other compensation for damages of defamation. Thus, it is reasonably clear that damages in cases of misuse of private information are awarded to compensate the claimant for the hurt feelings and distress caused by the misuse of their information.

From the discussion above, it is notable that the main privacy principles in the EC Directive on Data Protection are 'notification', 'choice', 'security', 'data integrity' and 'accessibility' and 'accountability'. However, it does not include the principle of 'enforceability', which is recommended by the US Federal Trade Commission (FTC) in the EU–US Safe Harbour Agreement. Enforcement of privacy protection is one of the most complicated

issues in information privacy protection. The legal certainty of enforcement of privacy protection is vital to build Internet users' trust on web systems. Before the discussion on enhancing enforceability of privacy protection, the linking factor to be looked at is whether the current computing technologies are compatible with the legal framework of the data and privacy protection.

3. Privacy and security with software agents and service-oriented computing

3.1. *Overview of current technologies*

Recent widespread growth in the number and complexity of distributed systems in dynamic business environments has lead to the creation of sophisticated tools and technologies to support the design, development and management of automated transaction systems that are integrated with data and privacy protection. Two technologies in particular, namely agent-based systems and service-oriented computing, stand out as being able to support the required autonomy, flexibility, proactive and reactive characteristics in dynamic business environments. At the same time, agent-based systems and service-oriented computing can generate a secure system that provides the protection of personal data and privacy. Agent-based systems can establish and adopt certain personal data and privacy protection rules, while service-oriented computing offers a promising solution in discovering other appropriate agents, reaching agreements between service providers and customers, managing the joint execution of tasks and dealing with any problems that arise.

The term 'agent' has been widely used in the computing industry and although there is no single precise definition, most researchers and practitioners accept the definition proposed by Shoham, that an agent is 'a software entity which functions continuously and autonomously in a particular environment, often inhabited by other agents and processes'.[7] Agents typically act on behalf of a user, which might be an individual, an organisation, or even another agent. Wooldridge captures this aspect by defining an agent to be, 'a computer system that is situated in some environment, and that is capable of autonomous actions in this environment in order to meet its delegated objectives'.[8] Software agents can be characterised by the properties of autonomy, reactivity, proactiveness and social ability. Autonomy implies that agents are able of making their own decisions and although they may be influenced by others, an individual agent has the ultimate control over its own behaviour. Agents are reactive in that they monitor their environment and circumstances, and are able to change their behaviour accordingly. Similarly, agents are able to identify and create opportunities by acting proactively, in order to fulfil their goals. Finally, agents are able to coordinate their actions with others in order to cooperate, to enable them to achieve goals that could not, or not as easily, be achieved alone. Groups of agents can organise themselves by establishing and adopting certain rules, or norms, with minimum human intervention then required for them to achieve their design goals. Such cooperation and coordination requires agents to be able to discover other appropriate agents, reach agreements with other agents or with customers, manage the joint execution of tasks and deal with any problems that arise. There are several alternative approaches and technologies for designing and implementing such systems, but there is currently no single generally adopted standard. Of the possible approaches, the tools and technologies provided by service-oriented computing offer a promising solution.

'Service-oriented computing' (SOC), also known as 'service-oriented architectures' (SOAs), is a paradigm for distributed system development that allows software developers to focus on the fulfilment of the required enterprise functionalities at a conceptual level

through the provision of standardised communication protocols, interfaces, workflows and service management infrastructures. SOC allows developers to build the functionality that they require by combining existing components, called services, without being concerned by the barriers of heterogeneous operating systems, hardware environments, development platforms or geographical location.

Although the notion of SOAs is backed by numerous organisations, a number of varying definitions have been proposed by a selection of industry bodies, researchers and standards organisations. The World Wide Web Consortium (W3C) defines a service as, 'an abstract resource that represents a capability of performing tasks that represents a coherent functionality from the point of view of provider entities and requester entities'.[9] The key point in this definition is that a service provider is able to package specific functionality in a suitable format for consumption by a requester. IBM defines SOAs as, 'an approach to build distributed systems that deliver application functionality as services to end-user applications or to build other services. SOA can be based on web services, but it may use other technologies instead'.[10] Web services are one of the more popular technologies that are used to implement SOAs, having received wide industrial support. Services can be primitive or can be built from other services through a process called composition. An important feature of composition is that the component services may be supplied by different providers. This aspect is captured by the definition used by the OASIS consortium, who defines SOAs as, 'a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations'.[11] A set of standards and metrics are therefore required for SOAs, so that services can be provided, consumed and evaluated in a consistent manner. Several alternative standards have been proposed for the various aspects of SOAs and although the technical details may differ between specific standards, the overall functionalities and characteristics defined are broadly similar.

Any system built using a SOA approach must implement a key set of processes, including advertisement, discovery, selection, composition and execution. A service provides certain functionality on behalf of its owner, which might be an individual or an organisation, and in order for a potential customer (the service requester) of the service to become aware of it, the service provider must advertise the service describing the functionality offered. Service providers advertise services by publishing service descriptions in publically available repositories, which are managed by service brokers (or registries) that are able to match customers' requirements with appropriate services. A customer submits their requirements for a given task to a broker, who will find suitable services and inform the customer of each potential provider's details, the service characteristics and information about how the service can be invoked. This process allows a customer to discover the available services for a given task and select the most appropriate. Once a service has been selected it can be invoked and executed. The composition process describes the manner in which new services can be created through the combination of existing services (potentially from several providers).

To remain competitive, and respond to market conditions, businesses frequently need to adapt their business processes and workflow, and this is one of the main motivations for SOAs, since their loose coupling of components is able to deliver this flexibility. Again, alternative standards have been proposed (such as ebXML and BPEL), but they share the overall functionality of enabling businesses to define orderings and constraints on a set of service invocations that include both their own services and those sourced from other suppliers. Since services are modular components any given service can be exchanged

for another that has the same description, thus enabling flexibility in the business process. Furthermore, since business processes are defined as ordered collections of independent components (i.e. services) they can be easily adapted by inserting or removing services or changing the ordering.

Since many providers can offer similar services, service requesters need some means of choosing between them based on non-functional attributes such as quality of service (QoS). The idea is that a customer can find the best set of services available at run-time, taking into consideration their preferences and the current execution context.[12] Where complex business processes have been defined individual service components can be selected at run-time according to QoS characteristics, and services that fail to meet their required characteristics can be replaced.

3.2. *Problems with widespread adoption*

The combination of agent-based systems and service-oriented computing allows complex business processes to be defined, and automatically managed by autonomous agents that can select appropriate services and even reconfigure business processes at run-time according to user preferences and QoS criteria.

However, in any service-oriented interaction, issues such as data and privacy protection still need to be addressed to ensure that all parties are appropriately protected in an agreement that also defines the non-functional commitments that each party should make. In other words, the agreement should include characteristics such as privacy and security in addition to standard aspects such as delivery times and payment terms. Privacy and security are complex issues, in which the requirements of protecting data and privacy are not straightforward to ensure or to define. For example, since services can be composed of other services provided by different suppliers, which may be selected at run-time, it is not necessarily known which provider will have access to a given user's data when the original agreement is made. Services often involve the execution of program code, which means that it is not necessarily known at the time of invoking the overarching service which provider (or sub-provider) will run the code, and so potentially have opportunity to copy or reverse engineer it or duplicate any associated data.

Most existing work in this area has focused on B2B interactions, where both the providers and customer of services are businesses. When a particular service is selected it is typical to establish the notion of a 'service contract' that defines the commitments made by the provider and customer (for example defining when a service will be performed, the security measures that should be in place and details of payment). Such 'contracts' may also give details of any penalties that are incurred in the event of commitments being broken. These 'contracts' exist at a technical level, and although they mirror the paper contracts that are exchanged between businesses, it is not always clear what legal standing they have. In existing deployments of SOAs the typical operation with respect to contracts is that an overarching legal agreement is negotiated and signed by human representatives of the organisations involved, and it is only the specific implementation (in terms of the composition of services within the particular agreed parameters and business processes) that are determined and executed online.

Over recent years there has been a trend towards customers being more directly involved in such interactions, both as providers and customers of products and services, and towards the interactions themselves being more flexible. Such a change has been witnessed in industries ranging from music and entertainment to manufacturing. For example, individuals can easily publish and consume music online without involving

record companies (e.g. through iTunes), or by using aggregators or 'brokers' can manufacture and sell very small runs of physical products (e.g. manufacturing via Alibaba.com and selling through specialist sites such as etsy.com).[13] There is every reason to expect that a similar shift will occur within SOAs, since at a technical level it is already straightforward for anyone to publish or consume services. One obstacle to such a paradigm shift and a potential problem should it occur, is that the model of human representatives of organisations defining a legal agreement within which their agents and services operate is impractical since (i) individuals are unlikely to have the resources to setup such agreements, and (ii) if there is a shift in service provision from small numbers of business-to-business 'high volume low margin' interactions to a large number of 'low volume high margin' interactions with customers then the number of agreements that a given provider would require to negotiate is likely to become intractable.

3.3. *Consideration*

From a technical perspective in terms of data and privacy protection, users can specify restrictions on which sub-providers may be involved in fulfilment of their tasks. Additionally, users may wish to specify 'sandboxing' requirements such that their tasks are performed in isolation to those of other users, to prevent a malicious user from submitting services whose aim is to collect information about the other services that a provider is currently executing.

The above consideration arises from the possible practice of SOA systems, that is, the existing SOA systems typically address the concerning issue of 'defining a legal agreement within which their agents and services operate' by using overarching legal agreements between humans. This practice, as it has been argued in the previous sub-section, was likely to be impractical if customers became more directly involved in the provision and consumption of services. There is therefore a need for the current approach to become more customer focused, to support the legal requirements that exist regarding privacy and security. It is uncertain exactly how this issue can be solved, but it is clear that some form of contractual agreement between provider and customer is required, be they human negotiated or automatically negotiated. In the short-term it may be possible to introduce a form of 'trustmark' for contracts, such that a provider can have their contracts approved by an independent third party who can then certify that sufficient protection for the customer (and provider) is in place. However, there are two significant limitations with this approach. First, it places a high barrier of entry to individuals wishing to provide services, since they would need to formulate an appropriate contract and have it validated. A potential solution to this would be to use a broker or proxy service that has template contracts that can be adopted (analogous to sellers adopting the privacy statement and practices and the buying and selling policies of sites such as eBay that in turn are certified by organisations such as TRUSTe), but it is unlikely that such template contracts can be made sufficiently broad to be practical and yet detailed enough to provide appropriate protection. Second, and more importantly, such contracts will be inflexible, requiring approval by the independent third party and unable to be updated rapidly in response to circumstances at run-time. One of the main advantages of SOAs is the flexibility with which services can be selected and configured at run-time according to user preferences and the current situation. Legal agreements, however, are typically fixed and so restrict flexibility, which goes against this motivation for using SOAs. The underlying technology supports flexible workflows and interactions, but these are not easily modelled using traditional legal agreements. A potential solution is software contracts, which mirror paper contracts

but are negotiated and agreed by computers. Since these are computer readable, they can be modified at run-time, and so provide the desired flexibility. However, a key question remains, namely, how are the legal agreements on data or privacy protection generated by SOAs enforceable?

4. Solution: enhancing enforceability

In general, privacy policies are enforced either by national enforcement authorities, alternative dispute resolutions or court litigation. Those national enforcement authorities can impose sanctions or fine for privacy breaches. In the UK, the enforcement authority is information commissioner, whereas in the USA, the enforcement authority is the federal trade commissioner. Cross-border data transfer and enforcement is one of the most complicated issues concerning the protection of personal data and privacy. There are bilateral and multilateral agreements about seeking to enhance and encourage cooperation between the countries on these matters. For instance, on 27 November 2009, the Council of the European Union issued the 'Decision on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (hereafter "Agreement")'.[14] The Agreement provided for its provisional application as from 1 February 2010.

Because it is time-consuming and complicated to enforce privacy protection in courts and it is even more complex when the dispute concerns cross-border data transfer, self-enforcement mechanisms in private sectors have been strongly encouraged. Both OECD 'Privacy Online: Policy and Practice Guidance' in 2003[15] and the FTC Fair Information Practices Report in 2000 found that fostering the adoption of self-regulatory enforcement mechanisms or initiatives, such as trustmark or seal programs, would be beneficial for promoting effective global solutions with regard to privacy compliance. The FTC Fair Information Practices Report stated that the 'industry's primary self-regulatory enforcement initiative has been the development of online privacy seal programs'.

A seal program, known as a 'trustmark', is usually accredited by a trusted third party and displayed on the authorised website. It is designed to build users' trust on using the authorised websites. It gives users certainty about the privacy policy standards with respect to the kind of information a site gathers, what the site operator does with that information, and with whom that information is shared. The well-known seal and trustmark programs are TRUSTe, BBBOnline and VeriSign. Several companies' websites have been licensed by such online privacy seal programs. For example, eBay and Microsoft are licensed by TRUSTe, Alibaba.com is accredited by VeriSign etc. However, current privacy seal programs are not widely supported by international and national legislation and only a relatively small percentage of sites have introduced online-privacy seal programs.

Both TRUSTe and BBBOnline have their own enforcement procedures: users filing a complaint and seal program providers responding to a complaint by imposing sanctions on accredited websites. Examples of such sanctions may include:

(1) requiring the Licensee to correct or modify personally identifiable information or change user preferences;
(2) requiring the Licensee to change its privacy statement or privacy practices; and/or

(3) requiring the Licensee to submit to a third-party audit of its practices to ensure the validity of its privacy statement and to ensure that it has implemented the corrective action required.[16]

However, seal program providers cannot require a Licensee to pay monetary damages or take further steps to exempt from legal violation. The complaint will be published except for pre-agreement on confidentiality. TRUSTe and BBBOnline are the sole judges of any dispute.

Mann and Winn recognised that this kind of complaint forum provided by TRUSTe and BBBOnline is an alternative dispute resolution (ADR) mechanism.[17] In the author's view, TRUSTe Watchdog Dispute Resolution Forum and BBBOnline Compliant Forum are not arbitration, mediation or negotiation as they are much lower than the standard of ADR procedures. This raises concerns on why TRUSTe and BBBOnline do not offer normal online dispute resolution (ODR) procedures using a standard ODR platform, where a complainant can file a case and appoint a neutral person such as an assisted negotiator, mediator or arbitrator to help resolve the case. TRUSTe and BBBOnline might save costs and avoid complication in the sole judgment, but it might be fairer, much more trustworthy, reliable and professional to adopt an efficient ODR procedure as cases of privacy breaches are usually not very simple and often require expert investigation.

Seal programs' ODR services can be provided by two possible means. The first method would be that seal program service providers could purchase or produce user-friendly ODR software and appoint qualified assisted negotiators, mediators and arbitrators. The second method would be that seal program service providers could form partnerships with independent ODR service providers and publish the appointment agreement that seal accredited privacy-policy disputes would be resolved by their ODR partner. It is worthy of noting that, as mentioned earlier, eBay is accredited by the TRUSTe seal program, while eBay users' disputes are compulsory to be resolved by SquareTrade (an ODR service provider) first before they go for litigation. In other words, eBay users have different channels to resolve different types of disputes, privacy-related issues on TRUSTe Watchdog Dispute Resolution Forum and business-related issues on SquareTrade. Under these circumstances, it might make sense that SquareTrade is also designated to resolve eBay Users' TRUSTe privacy-policy disputes to enhance the users' confidence in providing personal information to proceed with commercial transactions.

5. Concluding remarks

Trust and security are now, more than ever, critical issues in doing business, whether online or in the paper world. The development of global legislation in relation to data protection and information privacy becomes vital to facilitate international commerce.

One way to achieve legal certainty and predictability is through international harmonisation. Currently, the International, EU and US privacy legislation or guidelines have their different preferences. The EU legislation aims more at protecting individual privacy rights, while the US and International guidelines are more targeted at promoting the free flow of cross-border data for the development of global economy. There is one aspect in common, that is, they all make efforts on balance between individuals' privacy rights and entrepreneurs' marketing rights at the level of international harmonisation. Both legal and technological measures should be used to build a trusted environment and increase users' confidence in dealing with data and privacy. From a technological perspective, agent-based systems in combination with service-oriented computing can provide the design

for secure automated transactions and personal data protection, however, users should make sure that they use or draft restrictive data protection terms in computing service agreements to enhance such protection in place. From a legal perspective, trustmark program, provided by a trusted third party certifying the quality of merchants' data privacy, should be deemed to be one of the most effective approaches in enhancing users' trust and confidence in online interaction and transactions.

Notes

1. BBC Radio 4, 'High Frequently Trading', program number: 09VQ4560LH0, Tuesday 3 November 2009, 20.00–20.40.
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23 November 1995, P. 0031–0050.
3. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal* L 201, 31 July 2002, P. 0037–0047.
4. EDPS second Opinion on ePrivacy Directive review and security breach: privacy safeguards need to be strengthened, Press Release, Brussels, Monday 12 January 2009.
5. Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. C 128/33, 6 June 2009.
6. D. Cooper et al., 'Security Breach Notification in Europe on the Horizon', World Data Protection Report, October 2006.
7. Y. Shoham, 'An Overview of Agent-Oriented Programming', in *Software Agents* (Menlo Park, CA: AAAI Press, 1997).
8. M. Wooldridge, *Reasoning About Rational Agents* (Cambridge, MA: MIT Press, 2000).
9. D. Booth et al., 'Web Services Architecture', available at http://www.w3.org/TR/ws-arch/ (accessed 16 February 2010).
10. M. Colan, 'Service-Oriented Architecture Expands the Vision of Web Services, Part 1', available at http://www.ibm.com/developerworks/webservices/library/ws-soaintro.html (accessed 16 February 2010).
11. OASIS, 'OASIS Reference Architecture for SOA Foundation, Version 1.0', OASIS Public Review Draft 1, available at http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra-pr-01.pdf (accessed 16 February 2010).
12. S. Meng and F. Arbab, 'QoS-driven Service Selection and Composition', in *Proceedings of the 8th International Conference on Application of Concurrency to System Design*, Xi'an, China, 23–27 June 2008.
13. C. Anderson, 'Atoms are the New Bits – the New Industrial Revolution', *Wired (UK)*, March 2010, 76–85.
14. Council Decision (2009/.../CFSP/JHA) of on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, Council of the European Union, Brussels, 27 November 2009, 16110/09, JAI 838, USA 101, RELEX 1082, DATAPROTECT 73, ECOFIN 805.
15. OECD Working Party on Information Security and Privacy, 'Privacy Online: Policy and Practice Guidance', DSTI/ICCP/REG(2002)3/FINAL, 21 January 2003.
16. Group of Experts on Information Security and Privacy, 'Implementing the OECD "Privacy Guidelines" in Electronic Environment: Focus on the Internet', DSTI/ICCP/REG(97)6/FINAL, 9 September 1998.
17. R.J. Mann, *Electronic Commerce*, 2nd ed. (New York: Aspen Publishing, 2005), p. 227.