December 2002

# eConsent: A Critical Element of Trust in eBusiness

Roger Clarke
*Xamax Consultancy Pty Ltd, Australia, Department of Computer Science, Australian National University*

**15th Bled Electronic Commerce Conference**
**eReality: Constructing the eEconomy**
Bled, Slovenia, June 17 - 19, 2002

# eConsent: A Critical Element of Trust in eBusiness

**Roger Clarke**

Xamax Consultancy Pty Ltd, Australia
Department of Computer Science, Australian National University, Australia
Roger.Clarke@xamax.com.au

## Abstract

*Gradually, discussions about the mechanisms needed to achieve trust by consumers in e-business dealings are becoming more fine-grained. One element that has attracted almost no attention to date is the signification of consent within telecommunications-based systems. This paper examines the role of consent within the broader area of trust; identifies its dimensions; proposes a framework within which e-consent services can be conceived, designed and developed; and considers the scope for implementation.*

## 1. Introduction

Consent means acquiescence, permission or agreement. It can be approached as a question of human rights, of personal sovereignty, of self-determination and of ethics. It has been examined from the perspective of political economy (e.g. Herman & Chomsky 1988), politics (e.g. Glasser & Salmon 1995), public economics (e.g. Buchanan & Tullock 1962), and health care decision-making (e.g. Annas 1998), as well as in more specific contexts such as drug trials, inoculation, sexual harassment, rape and euthanasia.

This article examines the concept of consent, and applies it to the context of business generally, and especially to business conducted with the aid of electronic tools. The Internet's promise is being achieved only very slowly, and lack of trust has been identified as a major factor. Various aspects of trust have been examined

in the literature, including security and privacy. Consent has seldom been the focus of such discussions, and this paper sets out to fill that gap.

By e-business is meant all forms of electronic dealing among natural and legal persons, including e-commerce, e-government, e-publishing and electronic services delivery. It is relevant to dealings among all combinations of individuals, small business enterprises, large business enterprises and government agencies.

Consent is relevant in the business-to-business (B2B segment), but especially so in business-with-consumer Internet commerce (B2C). One driver has been the gradual realisation by consumer marketing organisations that people like to at least have the impression that companies respect their interests, and their personal data. Some corporations have gone further, and perceive competitive advantage from 'one-to-one relationships' with individual consumers (Peppers & Rogers 1993), and in 'permission-based marketing' as a means of improving relationships with their customers (e.g. MessageMedia 2001).

During the second half of the twentieth century, most advanced jurisdictions have enacted consumer protection legislation, reflecting the imbalance of power between corporations and individuals. In addition, most jurisdictions have, since about 1970, enacted laws that formally recognise consumers' interests in data about themselves. Many of these go so far as to impose some constraints on business activities, and to provide consumers with some legal rights. Most of them explicitly refer to consent as a factor in the handling of personal data. This substantial change in the relationships between individuals and organisations has arisen from a number of trends that were evident during the second half of the twentieth century, Those trends include the following:

- dealings between individuals and organisations are still increasing in their **data-intensity**, as organisations depend less and less on human contact and more and more on technology and computer-performed processes;
- the forces of globalisation, including in recent years the Internet, are giving rise to a yet greater degree of **alienation** between people and the institutions that they have dealings with;
- **surveillance technologies** are burgeoning, they are engendering consumer and citizen suspicion, and they are stimulating counter-measures;
- the emergence of mobile business has brought with it convergence among Internet access devices, and increased the scope for organisations to perform **person-identification, person-location and person-tracking** Clarke (1999e); and
- new generations of net-consumers may have been at least partly infected with **the cyberculture ethos**. If so, they are likely to utilise the Internet's potentials in order to form much more powerful and effective consumer coalitions than have existed in the past.

This paper commences by briefly surveying the concept of trust. It then examines the nature and dimensions of consent as a means of inculcating trust. This is followed by consideration of consent in the context of open public networks and e-business. A generic e-consent process is presented, the concept of an 'e-consent object' is introduced, and implementation possibilities are discussed.

## 2. Trust

When one party is dependent on the behaviour of another, uncertainties exist, which give rise to risks. In the physical world, risk-management techniques are institutionalised, and who bears which residual risks is reasonably well-known. Large organisations may seek to exercise their market power over relatively weak individuals and small business enterprises. In civilised countries, consumer protection laws provide some degree of counterbalance against such abuses of market power.

With the advent of marketspaces, new uncertainties have arisen, and new balances have to be sought. The other party is more difficult to identify and locate, and hence to pursue when things go wrong. Information provided is not easy to authenticate. The challenges are compounded by the manner in which cyberspace challenges conventional geographical jurisdictions.

With transactions in physical space, and even more so in electronic space, each party needs to tolerate some residual risks inherent in transactions. The notion of trust involves having confidence in the other parties, and hence having an expectation that the risks mostly will not result in loss. A useful working definition of trust is "**confident reliance by one party about the behaviour of other parties**".

The origins of the trust are in family and social settings, and the concept is tightly bound up with cultural affinities and inter-dependencies. Trust in the context of business, on the other hand, is not grounded in culture, but is merely what a party has to depend on when no other form of risk amelioration strategy is available.

Trust can be based on a direct relationship between the parties (such as a contract, or prior transactions); or on experience (such as a prior transaction, vicarious experience, or a trial transaction). When such relatively strong sources of trust are unavailable, it may be necessary to rely on 'referred trust', such as 'word-of-mouth', reputation, delegated contractual arrangements, or accreditation by some body considered to be itself reputable. The weakest bases for trust are mere brandnames, and meta-brands such as 'seals of approval' from organisations that are no better-known than the company they purport to be attesting to (Clarke 2001d). Examinations of trust include Gambetta (1988), Doney & Cannon (1997), Hoffman et al. (1999), Tan & Thoen W. (2000), Friedman et al. (2000), Schneiderman (2000), Koehn (2001), Cook (2001), Solomon & Flores (2001) and Clarke (2001h).

In the context of B2C, many organisations have carried over the 'consumer as prey' attitudes prevalent in the 'mass marketing' and 'direct marketing' eras. This is evidenced by successive failed or failing initiatives, such as billboards on the information superhighway (1994-95), closed electronic communities (1995-97), push technologies (1996-98), spam (1996-), infomediaries (1996-99), portals (1998-2000) and surreptitious data capture (1999-). These are examined in Clarke (1997a, 1997b, 1998a, 1998d, 1999a, 1999c).

Consumers continue to lack confidence in Internet commerce, and growth is slow. Examinations of various aspects of B2C, and guidelines on how to overcome the disastrous start to the B2C era, are offered in Clarke (2001a, 2001c, and 2001g). Central to these proposals to inculcate trust are the notions of consumer choice, permission-based marketing, and information provision to consumers in order to enable choice. Yet to date there has been far too little consideration of the concept and dynamics of consent.

## 3. Consent

In some circumstances, consent is irrelevant, because legal authority exists. In other circumstances, one party (usually the corporation) has sufficient market power that it can safely ignore the interests of the other (usually the consumer), and coerce their behaviour (Clarke 2001e).

On the other hand, even in the relatively *laissez faire* environment of the U.S.A., B2C activities are subject to some degree of regulation. One source is contract law, which enables the parties to define the undertakings each enters into, and to specify the terms of the agreement (subject to some terms that are implied). Many jurisdictions also provide explicit consumer protection laws, to reflect the disparity in the power relationships.

In many circumstances, however, consent is significant as a means of inculcating trust. Moreover, it was discovered to be so some years ago, e.g.: "consumers want full disclosure, full consent, opt-in" (Novak et al. 1997).

The following sub-sections examine the concept, contexts and characteristics of consent. Because of the paucity of experience in business and especially in e-business, the discussion draws ideas from sources in areas where the concept is far better developed, in particular health care settings.

### *3.1 Definition*

Dictionaries offer a wide array of meanings if the term 'consent'. An inspection of statutory law in which the term is used, on the other hand, locates few formal

definitions. Drawing together the elements that are apparent from the various sources, a working definition of consent is "concurrence by a party with an action to be taken by another party".

The basic concept appears to be generally independent of such questions as whether the concurrence is offered by the party giving it, or procured by the other party; whether the agreement is spontaneous, or is influenced by the other party; whether or not the party acquiring the consent offers inducements; and whether any inducements offered are of the nature of a reward or a penalty.

### 3.2 Contexts

Consent has relevance in a wide variety of contexts. Some are at a high level of abstraction, as in the (often tacit) consent that citizens give to governments to define and implement social policy, and to engage in acts of war. That kind of consent is not further considered in this paper.

Still mostly outside the domain of e-business, but more closely related, is consent by individuals to actions in relation to their person. Because this is a primary source of the available practical experience with consent, this paper pays considerable attention to it. Contexts include:

- **medical procedures**. The individual's consent is generally a pre-requisite to interventions such as the prescription of drugs, inoculation, and surgery;
- **acquisition and use of organs, body tissue and body fluids**. Generally, the removal of body parts, tissue and fluid from live people (e.g. donations of kidneys, bone marrow, blood and semen) is treated as a medical procedure. The removal of body parts and tissue from corpses is also in many countries predicated upon the consent of the individual given before death, or of next-of-kin given after death. In some countries, on the other hand, a deniable presumption of consent exists (including Austria, Belgium, France, Greece, Italy, Spain and Switzerland - see Wolfslast 1992); and
- **acquisition and testing of body tissue and body fluids**. Body tissue and body fluids are also used for diagnostics for health care purposes, and for substance abuse testing for law enforcement, for sporting regulation, and in some employment contexts. With exceptions authorised by law, the acquisition, and the testing, generally require the consent of the individual concerned.

A considerable body of law, policy and procedure exists, to regulate the manner in which the individual's agreement to such actions is acquired by health care professionals, law enforcement agencies, and where applicable such other parties as morgues and employers.

This existing body of law, policy and practice needs to be borne in mind when the diverse range of B2C e-business activities is considered, including such contexts as:

- promotion and marketing;
- contract terms and conditions;
- payments; and
- the handling of consumers' personal data.

In their **consumer marketing practices**, marketers commonly assume that they have an economically-justified right to invade the privacy of customers', prospects' and suspects' physical mail-boxes and email-boxes, and to intrude into their quiet enjoyment of their homes by calling them on the phone. Many consumers, on the other hand, assert that each of these practices should be permitted only with the individual's consent.

Under contract law, the **terms and conditions** that are applied to a transaction need to be offered, and accepted. Usually at least some aspects are likely to be expressly offered and accepted, although the courts might impute conventional terms of trade in any particular industry sector, and are very likely to regard some terms as being implied. In e-business contexts, explicit consent is conventionally achieved by the consumer clicking on an 'I accept' button in a web-form. An area of difficulty is the lack of consumer choice in such circumstances, because the only choice that exists is for the consumer to accept the fixed terms and conditions or not do business.

A further context is the **transfer of funds** from a consumer to a corporation. The dominant mechanism in Internet commerce is the use of credit card details to effect payment. In many cases, corporations do not merely use card details once and immediately delete them from their files, but rather store them in case there are subsequent transactions. This is not just a matter of convenience (avoiding re-keying and the associated risk of error), but also of security (avoiding further exposure of the details on an insecure medium such as email).

On the other hand, there is a problem of security of the details in the hands of the corporation, because the corporation itself, or its employees, might use them to generate further charges against the card. The question arises as to whether and how the consumer signifies consent for the first use of the details, for the retention of the details, and for subsequent uses of the details; whether and how the consumer discovers that any such actions have been taken without consent; and what recourse the consumer has when inappropriate actions have been taken.

Another crucial context is **consumer data management** by corporations, including its collection, its use, and its disclosure. Attention was drawn above to the tension between consumer and marketer perspectives concerning access to the individual's letter-box, telephone and e-mailbox. A similar tension exists in relation to personal data, because many consumer marketing companies treat it as though it were appropriable by them, for any purpose that suits them, at their choice.

Consumers are increasingly expecting, and demanding, less cavalier attitudes. Early data privacy laws in such countries as Sweden and Germany gave rise to the OECD's 1980 Guidelines. Most advanced western nations have enacted laws that regulate both public and private sector uses of personal data, and all have been heavily influenced by the OECD code. It is a limited form of protection that is commonly referred to as the 'fair information practices' model. The European Union has recently tightened its requirements, and declared its intention to protect its citizens' data against export to countries that do not provide equivalent protections (EU 1995). Some specific abuses are currently being singled out for attention, including spam and inappropriate use of cookies.

Alone among the economically advanced nations, the U.S. has resisted the enactment of a general law protecting consumers against the privacy-invasive practices of corporations, even though it has a vast array of context-specific legislation (Smith 2001, EPIC 2001). The combination of pressure from the European Union and the lack of trust by consumers has made it inevitable that some form of legal protections will be created and enforced (Clarke 1999b).

In 'fair information practices' laws, consent is important in several ways. In relation to data collection, they say that "The knowledge or consent of the data subject is as a rule essential ..." (OECD 1980, Collection Limitation Principle and para. 52). In addition, it is a vital means whereby limitations on use and disclosure of data are defined (Use Limitation Principle and para. 55).

Some kinds of consumer data are widely regarded as being particularly sensitive. Many organisations claim the need for access to **health consumer data**, despite the strong interests of individuals, and their claimed moral and even legal rights. Severe tensions exist between personal interests, those of other parties such as researchers and investigators, and in some cases the general public interest. In relation to the testing of body tissue and body fluids, for example, explicit consents may be needed for acquisition of the sample, for each test performed on the sample, for retention of the sample, for any re-testing of the sample, for the use of data arising from each test, for disclosure of data arising from each test, for retention of data arising from each test, and for the association of an identifier or pseudo-identifier with each sample and each item of data arising from each test.

Health consumer data intersects with B2C e-business, in that health care services are increasingly being conducted on the net, and health insurers are increasingly endeavouring to intrude themselves into the health care process.

At least the more affluent consumers generally regard protections relating to **taxation and financial data** as especially important. Another matter of considerable sensitivity is data that has historically been associated with severe prejudice, such as **gender, marital status, ethnicity and sexual preferences**. For a proportion of the population, **date and place of birth** are private matters, and the demands of organisations for that data are a source of considerable embarrassment. Concerns also arise in relation to **household data**. For example, the recording of gender and date-of-birth in such databases as electoral rolls can enable the ready identification of households without an adult male.

### *3.3 Characteristics*

A working definition of 'consent' was provided above. This sub-section submits the concept to more detailed examination. The organisation of this sub-section, and a reasonable proportion of the analysis, are original, because relevant literature is somewhat sparse and difficult to locate. See, however, Buchanan & Tullock (1962), Faden & Beauchamp (1986) and Hartnett (2000).

A critical issue is what constitutes evidence of consent. A range of possibilities exists. The most formal and reliable is **'express consent'**, where the individual provides explicit signification that they have granted it. Express consent may be **'consent in writing'** (including other recorded form, such as an email, or a tick in a box on a web-form). Consent may, however, be given in a manner that gives rise to **no record** (in particular, verbal or visual approval). The evidence in such instances is the recipient's notes, or memory, of the act of signification. See Bygrave (1998) for an explanation of the manner in which the German Teleservices Data Protection Act (Teledienstedatenschutzgesetz) of 1997 provides for teleservice users to be able to declare their consent electronically.

Weaker forms of evidence are available. The term **'implied consent'** is useful to refer to circumstances in which an individual's action (or perhaps inaction) reasonably causes another party to interpret consent as having been granted. For example, a person may provide information in a context in which it is clear that the information will be used for some purpose, or will be disclosed to some other person, e.g. a delivery address may need to be disclosed by a merchant to a courier company.

Unfortunately, the term 'implied consent' is also often used to encompass another, rather different circumstance. This is where a party infers from the context that the individual has given consent, but the inference is unreasonable or at least readily contestable. This is much more usefully described as '**inferred consent**'.

A further circumstance arises where the law creates a presumption that consent exists unless it is expressly over-ridden by the person concerned. In such cases, a person needs to be able to declare a **denial of consent**. This may also be express (in which case it involves a signification that may or may not give rise to a record), or it may be implied, or inferred.

To be effective, the act of consent needs to satisfy a number of conditions. An apparently valid consent may be found to be ineffective if the person does not have the **legal capacity** to give one. Considerable bodies of law relate to limitations on the capacity of children, people whose intellectual capacity is significantly impaired, the comatose, and the deceased.

Another requirement is for '**informed consent**', by which is meant that, for consent to be meaningful, the individual needs to understand its implications. See Hartnett (2000) for a treatment of the topic in the health care context. A consent must be specific and bounded. In particular, it must be clear from the expression, or at least from the context:

- what **action(s)** the consent authorises. This requires reasonable specificity in relation to, or example, the use of credit card details, and of the items of data it encompasses, from whom they are to be collected, by whom they are to be used, and to whom they are permitted to be disclosed;
- **to whom** the authorisation is provided. For example, is it given to a particular company, or merely a business unit within it, or also to related companies; and what happens in the event of a merger or takeover;
- for what **purpose(s)** the authorisation applies. Considerable difficulties arise from generalised expressions of purpose, such as a government agency stating 'for the performance of the agency's functions', and a company declaring 'marketing of goods and services'; and
- over what **time-period** it operates.

A further criterion used to judge whether a consent is effective is '**freely-given consent**'. This implies that no legal compulsion, duress, coercion or undue influence must be involved. There may, however, be inducements, or a *quid pro quo*. Indeed, contract law requires consideration to be provided by both parties as a pre-condition to the formation of a contract (and hence to the existence of a consent).

Additional vital features are the **revocability and variability** of consent, by the individual who gave it. Issues arise regarding the communication of the variation or revocation, and the notice required for it to take effect.

A further characteristic is the **delegability of the power** to consent. Relevant areas of law include guardianship, e.g. by persons *in loco parentis*, and powers of attorney. Particular challenges arise with the inference of power of attorney for the comatose, and especially for persons deemed to be 'brain-dead', and with 'enduring' or 'durable' powers of attorney, which are not voided by the person losing their legal capacity, e.g. as a result of senile dementia. Aspects that are relevant to B2B include the powers of directors and officers, and principal-agent relationships. Directly relevant to the B2C segment are procedures for persons who are too young to enter into an enforceable contract.

It is easy for a corporation to assert, or to simply assume, that it has the concurrence of a consumer to an action it proposes to take. This section has shown how difficult it can be to actually have that consent. Genuine permission-based marketing, contracting, payment and data-handling pose considerable challenges. The following sections consider how permission-based marketing can be enabled in the e-business context.

## 4. e-Consent

In e-business, a variety of circumstances exists in which one party wishes to provide consent, and it is only natural that the consent be provided using the same information infrastructure that supports the rest of the transaction. It would be unlikely that trust could be achieved by means of inferred, implied, or even express-but-unrecorded signification of consent. In the electronic context, express-in-'writing' signification is needed, in order to provide clear evidence. The following working definition is proposed: e-consent is "**signification by recorded electronic means of concurrence or otherwise with an action to be taken by another party**".

Consent is related to authentication. Authentication is commonly presumed to mean 'authentication of identity'; but this is not necessarily the case: **authentication** is a process whereby a degree of confidence in an assertion is established (Clarke 2001i). In some circumstances, the assertion is that a party has a particular identity, but in others the assertion relates to value, or to an attribute of a party, and not to the party's identity. The form of assertion to be authenticated that is relevant to this paper is '<a particular party> consents to <a particular action>'.

Consent is also related to **authorisation**, or privileges. This is conventionally used within computing systems to refer to a permission to access a resource such as particular data or a particular process. The permission may be based on legal authority, or power, or consent. The absence of permission may result in access to the resource being denied, or qualified; or in some additional action being taken, such as recording of the action taken and/or notification to some process or person performing a control role.

In order to facilitate trust in e-business, an e-consent mechanism needs to enable the following:

- declaration of the person's wishes;
- expression in some kind of record; and either
    - structured display of the consent to the recipient; or
    - programmatic protection of one of two kinds:
        - the prevention of access unless the specified conditions are satisfied (which is normally implied by the expressions 'authorisation' and 'access control'); or
        - less absolute protection, such as by the provision of access only after an explicit warning is displayed. This has application in the health care sector, where the ability for health carers to override access rules is important in order to enable the treatment of critically ill patients. Equally, however, controls are needed over abuses of the privileges, including education and training, warnings,

logging, exception-reporting of accesses, sanctions against abuses, and action against miscreants. It is not clear that this looser form of protection is appropriate in the B2C context.

An e-consent scheme must offer acceptable levels of **security**. Security refers to both a condition in which harm does not arise, despite the occurrence of threatening events, and a set of safeguards designed to achieve that condition. Threatening events are variously natural, accidental and intentional, and harm can be to persons, property, value, or reputation. Information security encompasses the whole of an information system, including organisational and individual behaviour, and manual elements of the overall system, as well as computing and communications aspects.

Moreover, security is important throughout the information life-cycle, i.e. during the collection, storage, processing, use and disclosure phases, and not merely the transmission phase so often focussed on in technical discussions of security. A comprehensive security strategy comprises a suite of inter-related safeguards structured in a hierarchical fashion, and dealing with infrastructure, threat management, vulnerability management, and application-specific security.

There is also a vital need for **compatibility with existing infrastructure**. This includes workstations, hosts, and local and wide-area networks; and protocols such as smtp/pop for email, ftp for file transfer, and http for fetching web-pages and submitting data via web-forms.

In addition, an e-Consent scheme needs to satisfy the following, more specific requirements:

- the scheme must exhibit **service integrity**, to ensure availability, reliability, completeness and promptness;
- each **facility** supporting participants in the system needs to be able to:
  - authenticate the identifier and/or attributes of other facilities; and
  - provide their identifier and/or attributes in such a manner that they can be authenticated by other facilities;
- **data** (including consent/denial, data that the consent applies to, and agent identifiers and attributes) needs to exhibit the following properties:
  - **data integrity**, to ensure that data is authentic, reliable, complete, unaltered and useable, and that the processes that operate on data are reliable, legally compliant, comprehensive, systematic, and protective of data;
  - **data access control**, to ensure that it is only available to those who should have it;
  - **authentication**, to ensure that appropriate checks are performed on data, identity and attributes; and
  - **non-repudiation**, to ensure that entities cannot convincingly deny important actions they have taken; and

- **the act of creating a consent** needs to satisfy the following conditions:
  - be provided by a person with the mental capacity to do so;
  - be provided by a person with the legal capacity to do so in respect of that action or data;
  - be express; or possibly reasonably implied, or (with great care) inferred, but in such a manner that an opportunity exists for the implied or inferred consent to be denied;
  - be informed;
  - be freely-given;
  - be specific and bounded;
  - be signified in a manner that provides evidence;
  - be non-repudiable (preventing the denial that the consent was given); and
- be variable and revocable, by means of a further transaction that satisfies all of the same conditions.

A comprehensive strategy is needed to ensure that the requirements are satisfied. Such a strategy needs to comprise:

- an **architecture** that provides a framework within which a cohesive set of safeguards can be devised and implemented;
- a **process**, to ensure that the strategy is articulated into a plan, and the plan implemented;
- **protocols and standards** to enable reliable interactions over public networks;
- **tools and tool-kits** to enable cost-effective and reliable implementation; and
- **resources**, to enable the design to be implemented.

This may seem to be a considerable set of requirements, and to be elaborate, costly or inconvenient to consumer marketing corporations. On the other hand, the provision of such facilities may prove to be a pre-condition for trust in e-business, and hence simply 'a cost of doing business'.

## 5. The e-Consent Process

An e-Consent scheme requires secure and reliable capture, communication and utilisation of the consent, among relevant human actors and their software agents. This section presents a model of the process involved, depicted graphically in Exhibit 1.

A context exists within which a process to produce a consent is initiated (process 1 in Exhibit 1). The initiation may be by either the person themselves or some other party, and may comprise a single step or an interactive process. Consent is then declared by the person concerned, using a computing facility, which comprises a computer with requisite systems software and application software (process 2). The consent is expressed in an e-consent object that enables it to be communicated to other parties (3). This may be by means of the transmission of a message to another party, or its storage in an accessible database or directory (4).

Either by receiving a message, or accessing the relevant database or directory, the e-consent object reaches a computing facility that is under the control of a person or application software. The consent may be subjected to some form of authentication (5). It may then be applied in some manner (6). Appropriate actions include a person reading it, or software using it to permit or deny access to a particular resource, or to warn a person about the lack of consent, or existence of a denial, relating to their permission to access a particular resource.

The e-consent object is conceptually distinct from the information that it refers to. The information itself could be included in the same message, or transmitted separately, or could be stored in a separately accessible database.

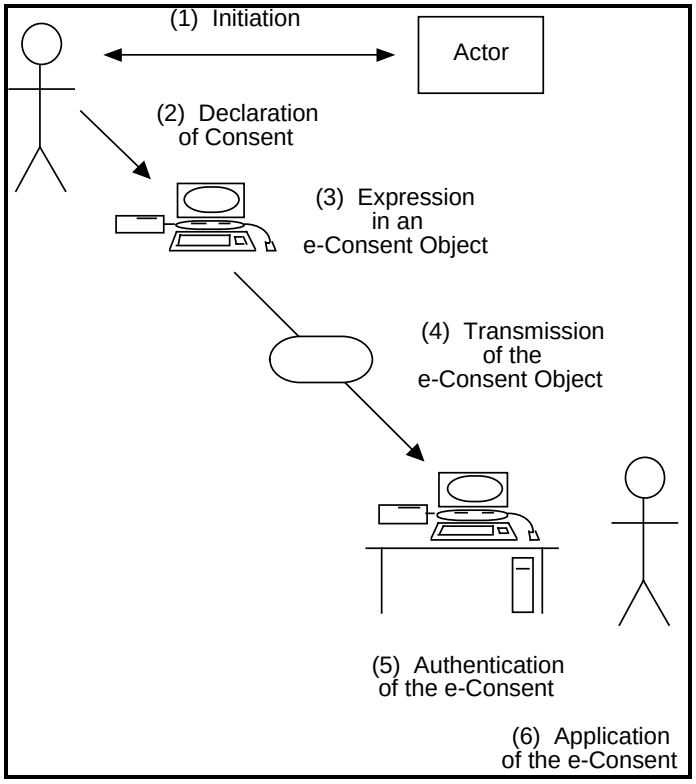


***Exhibit 1:*** *The e-Consent Process*

## 6. An e-Consent Object

The previous section identified the need for an e-consent object, as a means of encapsulating the data that defines the consent, together with any processes closely related to that data. This section provides an outline of what such an object needs to contain. A considerable number of data-items is involved, within a structure rather more complex than a simple list.

The purpose of the e-consent object is to provide a recipient with evidence of the consent, and to instruct a recipient as to what the implications of the consent are. A generic model of an e-consent object is an assertion of the following form:

> Access to <information>
>
> by <one or more entities or identities, or classes thereof>
>
> for <one or more purposes>
>
> in <a context>
>
> is [consented to | denied]
>
> by <an identity>

The information to which the consent relates might be designated by reference to one or more named objects, or as a set of data-items. In many contexts, definitions of the domains over which data-items are defined will also be challenging, especially in relation to the classes of entities.

In some circumstances, **supplementary data** may need to be supported. For example, where an agent acts on behalf of the individual, relevant data needs to be recorded about the agent, the power of attorney, and the circumstances. It may also be necessary to record the means whereby the person signified consent, and the date and time of expiry of the consent.

A consent clause may be subject to **qualifications**. For example, access might be granted to a general class of entity, but excluding some specific instance (e.g. all insurance companies except a particular one); and purpose might be expressed as the marketing of any of the company's goods and services except prophylactics. There may be multiple qualifications at each level. Hence the e-Consent object needs to support:

- a broadly-expressed consent;
  - qualified by one or more specific denials; and
- a broadly-expressed denial;
  - qualified by one or more specific consents.

The object needs to support **a hierarchy of qualifications**. An example drawn from the health care context is that a patient may:

- consent to the availability of all information to all health carers; but
  - within that, deny all information relating to HIV/AIDS; but

- within that, consent to information relating to HIV/AIDS to be available to STD clinics; and finally
  - within that, deny all information to a specific STD clinic (where Aunt Rosie works).

For revocation purposes, and to resolve disputes, an e-Consent object needs to contain **date-time stamps** that record when it was created and communicated, and this would need to be reliable and subject to authentication procedures.

Hence considerable care is needed in devising a data structure to support the e-consent object. Once again, this might be considered to be elaborate, costly, or inconvenient to the consumer marketing organisation; but it might well be a cost of doing B2C e-business.

## 7. Current Implementations of e-Consent

This paper has introduced the concept of e-consent, and proposed definitions, a process, and an object to encapsulate it. This section considers whether e-consent has been effectively implemented to date.

Some conventional web-site techniques are relevant. The most common is the presentation of terms of contract on a web-page, with an 'I accept' button that the consumer must click on in order to continue with the purchasing process. This inverts the expression of consent, because the statement is entirely pre-determined by the organisation seeking the consent. In many cases, the process fails against the criteria of being informed and freely-given consent. Various problems arise in relation to the power of the individual to provide the consent (e.g. lack of evidence that the person is not a minor).

The concept of 'info-mediaries' was introduced some years ago, to act as agents for collectives of individuals, and to interface on their behalf with consumer marketing organisations (Hagel & Rayport 1996, Hagel & Armstrong 1997). Notionally, these could be implemented using software agent technology. In practice, however, there is little evidence of info-mediaries actually emerging.

What has emerged is initiatives designed from the opposite direction, i.e. to serve the interests of consumer marketing organisations rather than those of consumers. An early proposal was Microsoft's Open Profiling Standard (OPS) which has given way to the company's generalised login scheme Passport and its associated centrally-stored 'wallet'. Competitor projects include AOL's Screen Name, AOL/Netscape's Quick Checkout, and the Liberty Alliance.

These initiatives, which are sometimes referred to as 'identity management' schemes, are strongly pro-marketer, evidence very limited involvement of consumer interests, are concerned primarily with the acquisition of approval from consumers, and give very little attention to specific, informed and freely-given consent, or even

security. For resources on the serious privacy-invasiveness of Microsoft's XP, .NET, Passport and wallet products and the intended Hailstorm / MyServices mechanism for web-services, see EPIC (2000-). Early in the second quarter of 2002, Microsoft switched its emphasis on MyServices from a Redmond-based service to a product to be sold to consumer marketing corporations. This is only a very marginal improvement in a parlous scheme.

A relevant protocol that originally held great promise is W3C's Platform for Privacy Preferences (P3P). The e-consent aspects of the protocol were still-born, however, and P3P is merely a means for web-sites to publish their privacy statements in a machine-readable format (Clarke 1998b, 1998c, 2001b). Extensions to P3P may emerge, which would enable it to graduate from a mere 'privacy policy publication protocol' to a genuinely privacy-protective software agent technology; but at present this seems unlikely.

## 8. Implementation Prospects

If e-consent is not currently implemented in a satisfactory manner, what more appropriate approaches are available? The following sub-sections examine each of the phases identified in Exhibit 1 above as being the elements of a comprehensive e-consent scheme.

### *8.1 Initiation*

An organisation may commence a process by contacting a consumer, e.g. with an offer to sell goods or services. Alternatively, a consumer may initiate. In some circumstances, an organisation is likely to declare that some aspects of the consent are non-negotiable. This is problematical, however, where the organisation has a monopoly, or the practices across an industry-sector are standardised rather than competitive. Mere recitation by the organisation of the fixed and pre-determined form of consent it requires does very little to inculcate trust. There would be considerable advantages if the process were capable of being interactive, to enable customisation of an e-consent object appropriate to the particular context. Hence interaction between the facilities of the consumer and the marketer is at least beneficial and possibly necessary.

The consumer and the marketer facilities need to have application software that use a common protocol (perhaps implemented in a web-browser plug-in and a web-server script, or by means of a web-form and/or an email-interchange). W3C's P3P protocol, although limited, does offer a means whereby an organisation can express its privacy policies in machine-readable form.

### 8.2 Declaration of Consent

The consumer could declare their agreement to the terms on their own computing facility, using email or a web-browser. The e-consent object could be created by either facility, provided that the contents and their implications were clear to the consumer, and not agreed to under duress, and hence consent was signified effectively.

If the consumer facility has the capability, the e-consent object could be digitally signed (preferably using a separate and secure token, such as a smartcard). Very few facilities used by consumers have such capabilities, however. In the absence of a smartcard and means to connect it, a less secure but workable arrangement would be for the consumer to indicate agreement to a consent form that replicates the contents of the e-consent object in a human-readable format. This could be displayed or printed, e.g. as a generated web-page, email or PDF document, and a copy retained on the consumer's facility.

The consumer's identity could be authenticated by keying a password / PIN / passphrase (or, if the importance warranted the trouble and expense, by signing and then mailing or faxing a printed version). In the physical world, organisations undertake limited authentication, and in many cases only do so where the matter is sensitive, or some grounds for suspicion of masquerade exists. A similar approach might be in many cases quite adequate in the digital world as well.

Other alternatives exist. A marketer might prepare an e-consent object on the basis of consent-related information already held on file. And circumstances exist in which the consumer is physically present in the office of the marketer or of an agent (such as a solicitor, accountant, financial adviser or health care professional). In such cases, the consumer can signify consent by such means as a signature on an office-copy of the printed document, or a keystroke on a computing facility within that office.

### 8.3 Expression in an e-Consent Object

The information needs to be expressed in an e-consent object that enables it to be communicated to other parties. An outline of such an object was provided in section 6 above. The object could be transmitted in a message, or stored as an entry in a database or directory.

If it is expressed as a message-format, then a candidate means for defining the format would be EDIFACT. In the present e-business context, however, XML would be a much more appropriate meta-language. If it is expressed as a database record, then various, mainly proprietary alternatives exist, but XML would be the preferable meta-language.

The information in an e-consent object is itself privacy-sensitive, and potentially highly so. Access to it therefore needs to be subject to security protections. This suggests that access controls need to be defined, and it may need to be stored in encrypted form on the consumer's facility, on the marketer's facility, on any other

facility that it may reside in, whether temporarily or long-term, and in any database or directory service.

### 8.4 Transmission of the e-Consent Object

For the e-consent object to be used, it must be communicated to other relevant facilities. Transmission security possibilities include the use of virtual private networks (VPNs), channel-encryption measures such as SSL/TLS, and message-encryption tools such as PGP.

### 8.5 Authentication of the e-Consent

The e-consent object may be subjected to some form of authentication. It is a large cluster of assertions, and it would need to be assessed which, if any, need to be checked.

The possibility exists of applying public key cryptography; but there are serious shortcomings in conventional approaches (Clarke 2001f, 2001j). The possibility also exists of applying smartcards or similar tokens, combined with passwords, PINs or passphrases, and perhaps biometrics.

Arrangements that may be less secure, but would certainly be less costly and more practicable, might be based on tokens bearing printed data, embossed data, bar-codes and/or data encoded into magnetic stripes. All such schemes require the issue and management of tokens, and authentication procedures to ensure they are not issued inappropriately. But they also require token-readers deployed in all relevant locations, which has to date represented a serious barrier.

As discussed in sub-section 8.2 above, simple userid/password pair techniques are currently the most sophisticated mechanism supported by mainstream computing facilities; and in some cases the individual granting the consent will not have an account, and may only be able to signify consent by indirect means.

### 8.6 Application of the e-Consent

The e-consent object needs to be applied to its purpose. One simple approach is for the contents of the e-consent object to be displayed to the person who seeks to take the relevant action. That person can then make a judgement as to whether or not they are permitted access.

This approach is insecure. In order to rein in abuses, controls would be important. The system could warn about the consequences of unauthorised access. Accesses could be logged, the logs routinely analysed, and exceptions reported in batch-mode or in real time to some monitor function (a person or a software agent). To be credible, such mechanisms need to lead to investigations of exceptions, and to the imposition of effective sanctions on those who abuse the privilege.

Such an approach would be considerably superior to the present very lax situation, and could be cost-effective in many circumstances in which the data is not overly sensitive, the access policies are provisional, or the consequences of false-rejection might be much higher than those of false-acceptance. Examples include manual overrides on dangerous equipment (such as chemical processes and fly-by-wire aircraft), and access to a patient's health care data in critical treatment contexts.

Much greater security is achieved where a system uses the e-consent object to permit or deny access to information. This is the function of access control (including role-based access control – RBAC), and is sometimes referred to as an 'authorisation' process, or a 'gatekeeper' function. See Weber (1999, pp. 378-391).

### *8.7 A Simple Implementation*

An example of a straightforward, practicable implementation is as follows:

- the marketer communicates the terms and conditions, or their requirements for personal information, by means of a web-page and/or in structured form;
- the consumer uses their computing facility to declare the consent they are prepared to provide, and to create an e-consent object. The consumer's facility might use an independent piece of software or a browser plug-in, together with a management tool for personal data and consents, perhaps combined with templates provided by a consumer or privacy association;
- the consumer uses their computing facility, together with adequately secure means such as SSL/TLS, to transmit the e-consent object to the marketer;
- the marketer's facility examines the e-consent object, to determine whether it satisfies the marketer's requirements. In the absence of an adequate protocol and tools, the inspection would be manual;
- if an agreement has been reached, the marketer's facility signifies this to the consumer's facility, and the marketer proceeds with the actions consented to by the consumer. Alternatively, the marketer declines the offer, or formulates and transmits a counter-proposal.

## 9. Conclusions

Consumers continue to be untrusting of Internet commerce, and the behaviour of e-marketers gives them every reason to stay that way. Trust in e-business would be greatly facilitated by a mechanism that enables consumers to express the terms of their consent, and to communicate that to other parties. This requires maturation beyond old-fashioned 'consumer-as-prey' marketing philosophies, and inversion of current thinking about 'identity management' and marketer-controlled declaration of terms and conditions, and storage of and control over personal data.

The purpose of this paper has been to contribute to the emergence of e-consent mechanisms. It has done so by examining the notion of consent in some depth; describing the process whereby e-consent can be declared, expressed, communicated and applied; and proposing some practical approaches to its implementation.

## Acknowledgements

The clarification of my ideas in relation to e-consent has taken place during the course of a lengthy project on its application to coordinated care, undertaken for the Australian Department of Health in Canberra. The project was conceived by Peter Broadhead, together with John Payne and team-members Jane Spittle and Kylie Jonasson. Other consultants involved in the project whose work has contributed to the framework have been Enrico Coiera of UNSW in Sydney and Christine O'Keefe of CSIRO in Melbourne. Of course, the ideas in this paper do not necessarily represent the views of the Australian Department of Health, nor of my colleagues in that project.

## References

Annas G.J. (1998) 'Some Choice: Law, Medicine, and the Market' Oxford University Press, 1998

Buchanan J.M. & Tullock G. (1962) 'The Calculus of Consent' Univ of Michigan Press, 1962

Bygrave L. (1998) 'Legislation and Guidelines: Germany's Teleservices Data Protection Act' Privacy Law & Policy Reporter 5, 3 (August 1998) 53, at http://www.austlii.edu.au/au/journals/PLPR/1998/56.html

Clarke R. (1997a) 'Cookies' February 1997, at http://www.anu.edu.au/people/Roger.Clarke/II/Cookies.html

Clarke R. (1997b) 'Spam' February 1997, at http://www.anu.edu.au/people/Roger.Clarke/II/Spam.html

Clarke R. (1998a) 'Direct Marketing and Privacy', Proc. AIC Conf. on the Direct Distribution of Financial Services, Sydney, 24 February 1998, at http://www.anu.edu.au/people/Roger.Clarke/DV/DirectMkting.html

Clarke R. (1998b) 'Platform for Privacy Preferences: An Overview' (April 1998), Privacy Law & Policy Reporter 5, 2 (July 1998) 35-39, at http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html

Clarke R. (1998c) 'Platform for Privacy Preferences: A Critique' (April 1998), Privacy Law & Policy Reporter 5, 3 (August 1998) 46-48, at http://www.anu.edu.au/people/Roger.Clarke/DV/P3PCrit.html

Clarke R. (1998d) 'Ad Code Must Respect Web Culture', The Australian, 15 December 1998, at http://www.anu.edu.au/people/Roger.Clarke/EC/ACS981215.html

Clarke R. (1999a) 'Key Issues in Electronic Commerce and Electronic Publishing' Proc. Conf. Information Online and On Disc 99, Sydney, 19 - 21 January 1999, at http://www.anu.edu.au/people/Roger.Clarke/EC/Issues98.html

Clarke R. (1999b) 'Internet Privacy Concerns Confirm the Case for Intervention', Commun. ACM 42, 2 (February 1999) 60-67, at http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html

Clarke R. (1999c) 'The Willingness of Net-Consumers to Pay: A Lack-of-Progress Report' Proc. 12th International Bled Electronic Commerce Conf., Bled, Slovenia, June 7 - 9, 1999, at http://www.anu.edu.au/people/Roger.Clarke/EC/WillPay.html

Clarke R. (1999d) 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice' Proc. User Identification & Privacy Protection Conference, Stockholm, 14-15 June 1999, at http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html

Clarke R. (1999e) 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications' Proc. 21st International Conference on Privacy and Personal Data Protection, Hong Kong, September 1999. Revised version in Information Technology & People 14, 2 (Summer 2001) 206-231, at http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html

Clarke R. (2001a) 'Of Trustworthiness and Pets: What Lawyers Haven't Done for e-Business' Proc. Pacific Rim Computer Law Conf., Sydney, February 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/PacRimCL01.html

Clarke R. (2001b) 'P3P Re-visited' Privacy Law & Policy Reporter 7, 10 (April 2001), at http://www.anu.edu.au/people/Roger.Clarke/DV/P3PRev.html

Clarke R. (2001c) 'Trust in Cyberspace: What eCommerce Doesn't Get' Proc. U.N.S.W. Continuing Legal Education Seminar on 'Cyberspace Regulation: eCommerce and Content', Sydney, May 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/TrustCLE01.html

Clarke R. (2001d) 'Meta-Brands' Privacy Law & Policy Reporter 7, 11 (May 2001) , at http://www.anu.edu.au/people/Roger.Clarke/DV/MetaBrands.html

Clarke R. (2001e) 'Towards a Taxonomy of B2B e-Commerce Schemes' Proc. 14th International EC Conf., Bled, Slovenia, 25-26 June 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/Bled01.html

Clarke R. (2001f) 'The Fundamental Inadequacies of Conventional Public Key Infrastructure' Proc. Conf. ECIS'2001, Bled, Slovenia, 27-29 June 2001, at http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html

Clarke R. (2001g) 'Privacy as a Means of Engendering Trust in Cyberspace' UNSW L. J., June 2001, at http://www.anu.edu.au/people/Roger.Clarke/DV/eTrust.html

Clarke R. (2001h) 'Trust in the Context of e-Business' at http://www.anu.edu.au/people/Roger.Clarke/EC/Trust.html

Clarke R. (2001i) 'Authentication: A Sufficiently Rich Model to Enable e-Business', at http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html

Clarke R. (2001j) 'The Re-Invention of Public Key Infrastructure', at http://www.anu.edu.au/people/Roger.Clarke/EC/PKIReinv.html

Cook K.S. (Eds.) (2001) 'Trust in Society' Russell Sage Foundation, 2001

Doney P. M., & Cannon J.P. (1997), "An Examination of the Nature of Trust in Buyer-Seller Relationships," Journal of Marketing 6 (1997) 35-51

EPIC (2000-) ' Sign Out of Passport!', at http://www.epic.org/privacy/consumer/microsoft/default.html

EPIC (2001) 'The Privacy Law Sourcebook – 2001' Electronic Privacy Information Centre, Washington DC, 2001

EU (1995) 'The Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data', European Commission, Brussels, 25 July 1995, at http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html

Faden R.R. & Beauchamp T.L. (1986) 'A History and Theory of Informed Consent' Oxford University Press, 1986

Friedman B., Kahn P. H. & Howe D. C. (2000) 'Trust Online' Commun. ACM 43, 12 (December 2000) 34-40

Gambetta D. (Ed.) 'Trust: Making and Breaking Cooperative Relations' Blackwell, 1988

Glasser T.L. & Salmon C. (Eds.) (1995) 'Public Opinion and the Communication of Consent' Guilford Press, 1995

Hagel J. & Rayport J.F. (1996) 'The Coming Battle for Customer Information' Harvard Business Review, 1996

Hagel J. & Armstrong A.G. (1997) 'Net Gain : Expanding Markets Through Virtual Communities', Harvard Business School, March 1997

Hartnett T. (Ed.) (2000) 'The Complete Guide to Informed Consent in Clinical Trials' PharmSource Information Services, Inc, 2000

Herman E.S. & Chomsky N. (1988) 'Manufacturing Consent : The Political Economy of the Mass Media' Pantheon Books, 1988

Hoffman D.L., Novak T.P. & Peralta M. (1999) 'Building consumer trust online' Commun. ACM 42, 4 (April 1999) 80-85

Koehn N.F. (2001) 'Brand New : How Entrepreneurs Earned Consumers' Trust from Wedgwood to Dell' Harvard Business School Press, 2001

MessageMedia (2001) 'Ten rules for permission-based e-mail marketing', at http://www.messagemedia.com/rc/ten_rules.pdf

Novak T.P., Donna L. Hoffman D.L. & Peralta M.A. (1997) 'Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web', Discussion Paper of November 9, 1997, prepared for the conference "Anonymous Communications on the Internet: Uses and Abuses" University of California Irvine, November 21-23, 1997, at http://www2000.ogsm.vanderbilt.edu/papers/anonymity/anonymity2_nov10.htm

OECD (1980) 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', Organisation for Economic Cooperation and Development, Paris, 1980, at http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-en.HTM

Peppers D. & Rogers M. (1993) 'The One to One Future : Building Relationships One Customer at a Time', Doubleday, 1993

Shneiderman B. (2000) 'Designing Trust Into Online Experiences' Commun. ACM 43, 12 (December 2000) 34-40

Solomon R. C. & Flores F. (2001) 'Building Trust in Business, Politics, Relationships, and Life' Oxford Univ Press, 2001

Smith R.E. (2001) 'Compilation of State and Federal Privacy Laws', Privacy Journal, Providence RI, 2001

Tan Y.-H. & Thoen W. (2000) 'Toward a Generic Model of Trust for Electronic Commerce' Int'l J. Electronic Commerce 5, 2 (Winter 2000-2001) 61

Weber R. (1999) 'Information Systems Control and Audit' Prentice-Hall, 1999

Wolfslast G. (1992) 'Legal aspects of organ transplantation: an overview of European law' Journal of Heart and Lung Transplantation 1992; 11 (4 part 2) 160-163