User Control Problems and Taking User Empowerment Further

Rowena Rodrigues

School of Law, University of Edinburgh
R.E.Rodrigues@sms.ed.ac.uk

Abstract. User control in identity management is beset with a number of problems, as outlined in this paper. It is argued that akin to traditional contexts, greater user control will result in greater user liability, which is demonstrated with the help of digital and non-digital examples. In this context, there is a critical need for greater user empowerment. This could be achieved in two ways– first, facilitating user awareness of identity management technologies, their scope and effects and second, through the implementation of proposed control-liability notices.

Keywords: User control, limitations of identity management systems, user liability, user empowerment, control-liability notice.

1 Introduction

User control in identity management refers to the power of the user[1] to determine and direct how one's digital identity, its attributes, relationships are created, constructed, maintained and decommissioned. It is a key factor of identity management; particularly in the user centric forms of identity management, which moot that individuals must be placed in greater control over their identities, attributes and identity relationships [1]. It is also hailed as one of the elements that determines the success or failure of an identity management system [2].

The user control approach to identity management is fraught with a number of problems. This paper examines such problems from the user's perspective. But the greatest challenge will potentially be the increase in user responsibility and liability, and in this light this problem is explored further. In this light it is suggested that users need to be empowered through greater awareness (public and private) and the implementation of control-liability notices.

2 The Problems of Control

2.1 Control – A Terminological Misnomer?

Technologists and identity providers' talk in terms of designing and providing solutions that help users control their identity. The use of the terminology of control is very

[1] In the context of this paper, the "user" refers to human beings.

V. Matyáš et al. (Eds.): The Future of Identity, IFIP AICT 298, pp. 211–225, 2009.

confusing at times. Different identity management technologists and providers conceptualise and implement identity management differently e.g. Sun Microsystems refers to identity management as its ability to help users "manage, audit, protect, share and store identity data" [3], the OpenID framework works more in terms of eliminating "the need for multiple usernames across different websites, simplifying your online experience" [4], Higgins speaks of enabling users and applications to integrate identity, profile, and relationship information across multiple data sources and protocols" [5].

Users, as individuals, expect different things from identity management systems in different contexts – organization of identities in some contexts, privacy or security in other contexts or a combination of all, in different measures. For instance, from a particular system they may require a high level of privacy with minimal data security [6], and from another simply a high level of data security. But, users and identity management providers do not always sing from the same hymn sheet. The difficulty arises when users fail to understand that different identity management systems offer varying levels and varieties of identity management since identity management is still by and large not a seamless experience across domains. Users may carry their expectations across domains, which may or may not adhere to common rules. Not all identity players play by the same rule and identity management systems are not restricted to local application (due to their global nature) whereas notions of control, privacy and security are.[2]

2.2 Control Not Primary Goal for Users

Controlling their digital identity is not per se, a primary goal for users. Using the Internet to network socially, seek information, make purchases, conduct banking transactions, and make travel arrangements, however may be. Managing one's identity on different websites or databases that hold personal data, profiles or other forms of identity is often less important than earning a living, writing up a thesis or caring for a sick family member. These are social facts that are often ignored in the user control debate.

The behaviour of users on social networking sites shows how users despite being given the technical possibility of protecting their profiles or personal information either do not bother to enforce stricter privacy settings or are sufficiently lax in their attitude towards taking steps in that direction [7].

Then again, control is a continuous and dynamic process. Users do not want to become constant vigilantes or puppeteers of their identity [8]. Nor can they effectively play this part indeterminately. Users are individuals with other and varied life contexts and any identity management solution must fit smoothly into these milieus and not disrupt them. Individuals simply will not adopt identity management solution enabling better user control if this is not the case.

2.3 Control Is Limited in Scope and Nature

Control is not and cannot be absolute. It is limited in nature and scope by various factors. Control, in terms of identity management, may not equate to effective identity security as opposed to what is repeatedly being told and sold to the users. Control

[2] Notions of identity control, privacy and security are still by and large culturally and jurisdictionally diverse, even taking into account the current state of technological globalisation.

may eliminate some risks, but the larger security issues still remain. The user of an identity management system is like the owner of a gun (indicative of identity). The gun owner keeps his gun in a combination safe (denoting an identity management system) – the combination of which is known to him and also to his wife, who he trusts. While this ensures that his children and other unauthorized people do not get hold of the gun and use it destructively or to his disadvantage, there is nothing to prevent his wife (who has access to the gun) from removing it from the safe and in a betrayal of trust using it for a violent or illegal purpose. A wife is well placed to compromise her husband's identity because she has intimate knowledge of his personal data or physical and behavioural identity.[3] Then again, a burglar could also break into the safe and steal the gun. An identity management system could, in similar manner, be internally or externally compromised.[4]

The ability to control may also be limited by factors such as whether one has the authority, power or means to control. One may not be able to control identity aspects or attributes one has not created or which are within the command of another and may be in that entity's interests not to relinquish control over. When identities are assigned or derived, control and ownership may lie elsewhere, and even if some form of limited control is possible, it may prove practically impossible, inconvenient or problematic. A simple example is one's identity or profile on a database. The identity or profile on the database may *relate* to me, but may not per se *belong* to me.

There may be a property interest in one's identity and its attributes and manifestations but one may be forced, coerced, inveigled or simply have to relinquish control for a number of reasons.[5] For instance, Google was ordered [9] to hand over to Viacom all data from the Logging database concerning each time a YouTube video had been viewed on the YouTube website or through embedding on a third-party website (including more importantly user names and IP addresses).[6] Users had no say or choice in the matter of this use of their personal information.

2.4 Ease, Convenience and Affordability

Another problem at the ergonomic level of identity management is that users will often resort to the "easy-quick-cheap" solution – a widely accepted view. It has been determined that if there is a trade off between risk and convenience, users "will take the easy option" [10]. For example, some digital users do not upgrade their anti-virus software because they find the process too complicated or get complacent. In the case of identity management systems, users may reject a high security system if they find that it is difficult to use or does not provide the desired level of interoperability or flexibility. Then again, they may resort to a convenient and easily accessible solution e.g. a fake anti-virus program they were directed to on the Internet [11].

[3] Or for instance, A's friend could create a fake profile for A with A's personal information that s/he is privy to. See Applause Store Productions Limited, Matthew Firsht v Grant Raphael, [2008] EWHC 1781 (QB); An identity management system might be similarly compromised by insider threats.

[4] E.g. through phishing, destruction and modification of data by malicious bots etc.

[5] E.g. employee digital identities or government/public authority created digital identities.

[6] This may have been implied in the Terms of Service, but it does not necessarily mean this would please users or that they would not feel a violation of their rights.

Affordability of solutions is also a factor that comes into play in securing and protecting identity. Users are often reluctant to invest money into security unless it is life threatening or visibly fraught with very serious consequences, e.g. many people now invest in shredders after becoming aware of how personal information is being used to facilitate fraud [12].

2.5 The “Human” Factor

The most important factor in user control of identity is “the human factor.” Users are individuals, groups, companies (made up of people). Users have different attributes – some users are more technology savvy, others less.[7] Some are young, some are old. Some are disclosure paranoid while others are disclosure prone. Erasmus, so eloquently stated that being human meant living in folly, erring, and being deceived [13]. This also applies excellently to the digital domain. Digital users are human beings who sometimes live in digital folly, make digital errors and get defrauded. They may forget email passwords and bank accounts. Users also may have vulnerabilities e.g. very young users, users with disabilities, users who need help to access the Internet or other digital technologies, or persons with mental impairments.[8]

Humans do not fully understand the intricacies and complexities of security (they do know what they want from security) and become expert at it through experience. Some may argue this is a naive assumption as people are generally adept at ensuring high security for that which they value. But, this assumes that people understand or are aware that there is a security problem (i.e. an identity threat or compromise, phishing attacks) and are empowered to act or deal with the problem. This also implies that when people weigh up an identity management system’s security they make a correct risk assessment in terms of how their digital identities will be treated and how secure they are.[9] This may often be more in terms of what they “perceive,” than what actually “is.”

2.6 The Illusion and Impossibility of Control and Security

Users’ over-reliance on technological measures and identity management systems might leave them more vulnerable through perpetuating illusions of control. What they see or get, may not be equivalent to what they think they are getting. If identity management systems are only effective in giving users a semblance of control, this is not going to be successful in helping users control their identity.

Use of identity management systems may lull users into a false sense of security. Risk and trust issues may remain unaddressed. For example, some identity management

[7] In a survey carried out in the United Kingdom, it was found that 56% of users found the Internet to be complex and 35% found it frustrating to work with. See W Dutton & E Helsper, “The Internet in Britain 2007,” OxIS Oxford Internet Surveys, University of Oxford, 2007.

[8] We must also take into account individuals who chose not to lead technologically oriented lifestyles.

[9] A risk assessment is dependant on a number of factors and presupposes effective forseeability of value of data and possible harms. A view supported by L Edwards & G Howells, “Anonymity, Consumers and the Internet: Where everyone knows you’re a dog,” in Digital Anonymity and the Law, C Nicoll et al (eds.), Chapter 10, p 207-248 at 242, (2003).

systems are vulnerable to phishing attacks and an attacker could capture a person's credentials or "sniff" out where the person's logs in [14]. Also, the user needs to "trust" the identity provider.

Security in identity management is a big challenge in itself [15]. Technologists constantly grapple with fixing bugs, while code-breakers and hackers continue to wreck havoc with the systems they design. There can never be 100% security, [16] although an optimal level of security can be sought to be achieved. There are intrinsic challenges in controlling security breaches and unauthorised access to identities and identifiable information [17]. Machines can be compromised by key loggers, trojans, viruses, malware and spyware.

2.7 The Merging of Actors; The Fusing of the Worlds

Technologies have brought about the merging of actors (state and private)[10] in a fusion of worlds (digital and offline). This is not a problem except for the fact that individuals often need to separate aspects of their identities according to contexts and purposes. User control is not only about controlling how private companies deal with one's digital identity but also about protecting one's identity from other individuals who are active participants in the identity stakes. With the merging of private and state interests in identity management and regulation both online and offline, user control takes on new dimensions.

Certain traditional forms of user control no longer remain singly effective. It is for this reason one can question whether technology (or for that matter norms or market)[11] by itself will be able to sufficiently support the user control his/her identity interests. And perhaps, it does make sense not to casually dismiss the part that perhaps the law could play in such a case.[12]

2.8 The Problematic "Privacy" Dimension

Identity management systems embody privacy and data protection norms as a primary means of protecting and enabling users' greater identity control. Identity and privacy have been deeply meshed, but there are some challenges to this approach, as explained below:

2.8.1 The Philosophy, Expectations and Implementations of Privacy Vary

Privacy arguably is as much a cultural concept (it is generally recognised as a western philosophical concept) as it is a legal one [18]. It has been interpreted differently in different countries and assumes different connotations for different people [19]. The expectations of people of privacy are as different as is the enforcement of the law on

[10] The merging of private actors happens on a constant basis – e.g. Yahoo and Flickr in 2005, Google and YouTube in 2006, LiveJournal and SUP in 2007.

[11] As postulated by L Lessig in Code and Other Laws of Cyberspace, New York, Basic Books, (1999).

[12] We acknowledge the call for a right to identity to protect individuals' identity. See P De Hert, "A right to identity to face the Internet of things," Ethics and Human Rights in the Information Society, 13-14 September 2007, Strasbourg, http://portal.unseco.org/ci/en/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf (2008).

privacy. In countries like India, where sharing of information is a common age-old and modern practice, informational privacy is virtually non-existent and the right to privacy developed through its judicial reading into the constitutional right to life.[13] There are fundamental differences between the philosophy of privacy of the United States and the European Union [20]. De Boni and Prigmore reported that in relation to the Internet, "current approaches to privacy are culturally biased, reflecting only one of a number of possible standpoints" [21].

2.8.2 Privacy's Out of Favour

While many people have come to value privacy as a fundamental right,[14] governments do not seem to like privacy.[15] A review of privacy rankings by Privacy International illustrates this very clearly [22]. Brazil, China, India, Japan, Russia, South Africa and the USA were amongst the worst for privacy enforcement. Also considered worst in regards to communication interception were China, Greece, India, Italy, Russia, United Kingdom and the USA amongst others. One EU law report goes so far as to state, "governments are even promoting privacy-invasive tools in fields such as e-government."[16] There is extensive documentation and evidence of pervasive surveillance even among privacy oriented societies like the UK.[17] Justifications range from national security interests, to public order, public health and law enforcement [23].

There is a common argument made that one cannot have privacy if one wants security. States use the national security clause to do away with aspects of what is private and such that is shielded as private. This is because of the widespread belief and fact that criminals (and terrorists) shield themselves and their actions in cloaks of secrecy and anonymity. Thus, we can see that enforcing strict privacy standards through technological means can pose a problem and conflict with the general public interest.

2.8.3 Consent and (Informed) Choice – Still Knotty Issues

Privacy (and data protection) balances on two important elements: consent and choice (read informed consent and choice). Most identity management solutions are premised on this. Both consent and choice have been rather problematic in the data protection domain. An examination of the implementation and working of other choice based mechanisms like P3P will show that these have not worked optimally in protecting the interests of the users. This may be because systems are often designed with a "smart user" (a powerful or expert computer user) [24] in mind. But users often are not "smart," "sophisticated" or even "reasonable" enough to enable them make the "right"

[13] Article 21, Constitution of India.

[14] Article 12 of the Universal Declaration of Human Rights, Article 17 International Covenant on Civil and Political Rights, See EU Charter of Fundamental Rights of the European Union - Article 7 and 8.

[15] Some writers make the case for limits on privacy – see A Etzioni, The Limits of Privacy, Basic Books, (2000) and D Brin, The Transparent Society, Basic Books, (1999).

[16] Main outcomes of the technical workshop on Privacy-Enhancing Technologies, 4 July 2003 http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/pet/200304-pet-outcome_en.pdf; see also L Cranor, "The Role of Privacy Enhancing Technologies, in Considering Consumer Privacy: A Resource for Policymakers and Practitioners, P Bruening (ed.), Center for Democracy and Technology, (March 2003).

[17] See the UK ICO's Surveillance Society Report 2006 and its May 2007 follow up at www.ico.gov.uk

or “necessary” choices. [25] They may not even have a choice in some cases e.g. if they wish to avail of a service they may have to consent or be deprived of the service. Often, they are not given a free choice (e.g. restriction on cross domain migration of avatars) or may be forced to make a choice to avail of a service they crucially depend upon. Other similar restrictions on behaviour may negate choice and action.

The “consent” aspect is a challenge too. Sherwin states, “…no one is sure just what consent is” [26]. Westen in similar vein stresses that when consent as a legal term has different meanings depending on the thing that is being consented to and the consequences of its non-existence [27].

From the above, we can infer that privacy laden user control approaches to identity management are inherently problematic given that privacy is coloured with cultural differences, there is strong state resistance to individual control and informed consent and choice, while widely deployed, remain complicated in practice.

2.9 Increase in User Liability

The problems with control are not only those inherent in its nature. There are also consequences that arise from control. Already most identity based service providers like Yahoo,[18] LiveJournal,[19] and Google[20] contractually provide that users are responsible for their actions and omissions.

The legal field is rich testing ground for the hypothesis that greater control results in greater liability, for example - command responsibility, parental responsibility, employer liability etc. In these cases, a right to control implies a duty to control and the responsibility for any consequent liability. A basic principle in law is that if one has a legal right of control and one ought to be in control, liability can be imposed whether or not the person concerned was in actual control [28].

Here are some further examples that reinforce the claim that the greater the user control, the greater the responsibility and liability.

2.9.1 E-Commerce

Perhaps the most germane example to illustrate how increased user control leads to increased user liability is the deployment of Chip and PIN cards in the UK.[21] The implementation of Chip and PIN[22] cards has meant that while users of such cards have gained extra security against misuse of their cards, they have acquired a corresponding responsibility and a duty to act with reasonable care towards safeguarding the cards and the PINs. Users have to take care of their cards, keep their PIN separate from the card, memorise their PIN, not write it down, not give it to anyone else, change it from time to time, not keep the card and PIN in one place, shield their entry of the PIN onto any PIN pad from shoulder surfers or security web cameras etc.

[18] See Yahoo! Terms of Service at http://uk.docs.yahoo.com/info/terms.html, specifically Terms Nos. 5 & 6.

[19] Live Journal Terms of Service at http://www.livejournal.com/legal/tos.bml, see terms IV, XIV and XVI.

[20] See Google Terms of Service, http://www.google.com/accounts/TOS?hl=en, Terms 5, 6 and 8.

[21] A Chip and PIN card means “a chip card that uses PIN as the preferred method of Cardholder verification at the point-of-sale (not only at ATMs),” http://www.chipandpin.co.uk/

[22] Personal Identification Number.

2.9.2 Data Protection Law

Data protection law imposes obligations and liabilities for all those who fall within the scope of the definition of "data controllers."[23] Directive 95/46/EC [29] prescribes the responsibilities and mandates for data controllers. A data controller must process personal data fairly and in compliance with the principles as enshrined in law, e.g. data must be processed fairly, lawfully, for a limited purpose. Individuals, it has been suggested, can be brought within the ambit of data protection legislation within certain limitations [30]. The *Bodil Lindqvist* judgment supports this principle [31]. In this case, a catechist in Sweden who had set up Internet pages permitting parishioners to obtain information from web pages containing information like people's full names, telephone numbers, hobbies, medical conditions, was held to have processed personal data within the meaning of the Article 3(1) of Directive 95/46/EC. This judgment thus shows that if an individual has control over identifying information (i.e. personal data); they incur a responsibility to act in accordance with established law and become accordingly liable for their actions or omissions. Users of identity management systems must then be similarly responsible, amongst other things, for the accuracy of their data, for maintaining the confidentiality of their accounts and passwords, notification of any breaches, security of their computer systems or they could cause themselves harm by becoming vulnerable to the effects of doing otherwise, as identity management companies would be inclined to shrug off any liability on the grounds that the user had not complied with reasonable expected practices, most of which are already embodied in most prevailing Terms of Service.

2.9.3 Intellectual Property Law

There are also intellectual property law cases that illustrate how control results in liability. For e.g. in *MGM v Grokster* [32], a case relating to whether distributors of P2P file sharing software[24] could be held liable for copyright infringement by users, it was held that the respondents "could not be held liable under a vicarious infringement theory because they did not monitor or control the software's use, had no agreed-upon right or current ability to supervise its use, and had no independent duty to police infringement" [33]. Grokster and StreamCast did not "operate and design" an integrated service of monitoring and control, they were decentralised and it was more of the users responsibility. But, the fact that it was the user who was "in control" in the P2P system of file sharing was certainly a contributory factor that led to widespread suits against individual file sharers by the music industry [34].

In another case, a lawsuit was filed by a leading business news organization against an investment group (and its employees) for unspecified damages for copyright infringement and violation of computer fraud and abuse law [35]. It is alleged

[23] Defined in Article 2(d) of Directive 95/46/EC as "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

[24] Peer to peer (or P2P) file sharing enables "users to share files online through an informal network of computers running the same software," http://www.onguardonline.gov/topics/p2p-security.aspx

that a single account set up by one of the investment group's employee was used by multiple persons on its US and non US-based network servers, other than the account holder to access articles on the news site. If this action succeeds, a clear liability will arise particularly for companies that permit or do not monitor how employees use their login ids.

2.9.4 Property Law

If we analyse the relationship between a landlord and his tenant there are some interesting observations to be made to support our user-control and liability hypothesis. A tenant is liable for his or her activities in the place of occupation after he or she is put in control of the premises. Conditions of lease or rental agreement make this very clear. There are also regulations that support this premise.

An identity management company/provider is like a landlord. Users are akin to tenants. When they use the services of identity providers they enter into a contractual relationship with the company and a legally binding relationship comes about much like that of the landlord and tenant.[25] There is one significant difference however. While a tenant is generally aware of his rights and responsibilities (either by virtue of tenancy agreements and terms becoming streamlined, commonplace or because tenants are aware of the dangers of entering into such relationship without reviewing terms that may go against them), the same may not be true of users who use the services of identity management companies or providers. Hitting the "I accept" button of terms of service without reading the full terms and conditions that are binding has become bit of a standard practice amongst users of Internet based services.

The tenant as occupier of the premises may also have other responsibilities – e.g. shielding other people on the property from any harm that is foreseeable,[26] or even making sure that he or she does not take any unreasonable measures to stop people venturing into the property or premises and must even take steps to warn of any harm that might be caused by erecting signs etc.[36] Users are similarly being provided with the means to erect digital fences for their identity and this means that they will have to ensure that they do make use of these means as a consequent duty has now become attached to them. This will mean that they will have to take due care and be responsible for what happens within the boundaries of their digital identity fence or any effects caused thereby.[27]

2.9.5 Tort Law

Since the relationship of the identity management systems and users has been compared to that of a car manufacturer and car driver by a certain section of the identity management industry [37], it is relevant to examine this relationship further in the light of its legal implications.

A car manufacturer designs the car. A prospective driver buys the car. The driver may have bought the car because it was popular, of a particular model, gave good mileage, was recommended or for any other reason. The driver uses the car to get from one destination to another.

[25] What this analogy mostly relates to are cases where identity providers provide users with identity that users may be in possession and use of but ultimately do not have ownership rights to.

[26] See the UK Occupier's Liability Act 1984.

[27] E.g. as explained in 2.9.2.

The driver controls the car. He starts it and keeps it going at whatever pace is required. He uses the steering wheel, the gears, and the brakes in the process. There are certain norms and rules that the car driver must respect while driving the car. He must ensure that he wears a seat belt (for his own safety), drive at a safe speed, show respect to other users, ensure that the car is in working order. He is expected to be reasonable, prudent and careful. The law imposes a duty on the car driver – a duty of caution and care and if he fails to exercise that caution and care, the driver will be responsible for any consequences that result and will be held liable.

Similarly, the user of an identity management system will be expected to use the identity management system appropriately, adhere to its norms, and understand its limitations. But just as there are good, average and bad drivers, the same is the case for users of identity management systems. Just like drivers, users of identity management systems may be inexperienced, alcoholic, drugged, distracted, drowsy, fatigued or simply reckless in their digital behaviour.

A driver is also required to maintain the car. However, in a case there is a mechanical defect in the car and the driver was unaware of the same, he may have a defence in law to any prosecution that arises [38]. Similarly, if there are circumstances beyond the control of the driver that lead him to lose control of the car, the driver may also successfully plead a defence e.g. nails on the road, stormy weather [39]. Thus, while there may be mitigating circumstances to allow a driver to escape liability, if it can be successfully proved that s/he had control over the car and/or knowingly broke the rules s/he will be made accountable for their actions.

The above examples show how liability follows control or is the flip side of control. In the long run, as identity management systems give more and more control to the user, the user will also acquire greater liability for actions or omissions in regard to the use of such systems.[28] Therefore, there is a pressing need to empower users, the biggest stakeholders in the identity management stakes.

3 Empowering Users

There are two key factors in effective control, which also extend in application to the digital realm: awareness and action. This section focuses primarily on the awareness aspect, which as currently being implemented leaves much to be desired.

3.1 User Awareness

Only if the user is aware of how control in identity management system truly works, its true scope, limits and the associated the obligations and liabilities, will user control be truly effective. Raising awareness has been a key focus of the data protection regime, and a number of steps have been and are undertaken in this light: e.g. establishment of a Data Protection Day, national data protection authorities undertake

[28] In this light see Recommendation 7 in R Anderson, R Böhme, R Clayton & T Moore, “Security, Economics and the Internal Market,” http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf (2008).

publicity exercises. But does awareness work or is it optimally working? Apparently not [40]. Even the Council of Europe website acknowledges that, "it is a well-known fact that European citizens are generally unfamiliar with data protection issues and unaware of their rights in this respect" [41].

Awareness is the condition of "being aware" or "conscious,"[29] a relative state of understanding or knowing (fully, reasonably or partially), which may or may not form the basis of rational action. There is a pressing need for increasing responsible public and private awareness of identity management systems be it through public information, education, media broadcasts etc. The results of the many excellent research studies into identity management systems, their scope, limitations and advantages need to be simplified and disseminated to wider audiences – something the academic community must take charge of, to do away with current limited approaches which are largely subject to different biases.

3.2 Proposal for a Control-Liability Notice[30]

There is a pressing need for identity management companies to assert and inform users of what levels of control a particular identity management system offers and what its remits and limitations are and also make clear that the use of identity management systems will leave them open to greater responsibility and liability. This must be done in an explicit, clear and concise manner, unlike long-winded privacy policies or Terms of Service that people hardly ever read[31] or do not read in entirety. There is a vital need to simmer complexities into simplicity.

The Article 29 Data Protection Working Party set up under Article 29 of Directive 95/46/EC proposed a layered approach to data protection notices: *short, condensed and full* [42]. This may be a good place to start. The UK Information Commissioner's Office has given guidance over what an effective data protection "notice" should constitute and this could be adapted and used as a template for a "control-liability" notice. A draft format is outlined in Figure 1.

This notice[32] could be placed prominently and must be aimed at general users not shrouded in legal terminology and aimed at legal experts. Such notices could have an embedded code that makes them quickly readable and acceptable line by line before users can proceed to the actual use of the application.

[29] See the Oxford English Dictionary. Aware has also been defined as meaning: watchful, vigilant, cautious, on one's guard, informed, cognizant, conscious, sensible.

[30] At this stage, this is a working proposal, a full analysis is out with the limited scope of this paper.

[31] The general view is that Privacy policies and Terms of Service are quite complicated and shrouded in legal jargon and not at all aimed effectively at users, rather in attempting to meet the legal requirement they have failed on this ground. See A McDonald & L Cranor, "The Cost of Reading Privacy Policies," The 36th Research Conference on Communication, Information, and Internet Policy, 26-28 September 2008; V Arlington & I Pollach, "What's wrong with online privacy policies?" Communications of the ACM, Vol. 50, Issue 9, pp 103-108, at 107, (September 2007) and G Milne and M Culnan, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices" J. Interactive Marketing, 18, 3, pp. 15–29, (Summer 2004).

[32] We acknowledge the limitations and challenges of notices in putting forth this proposal.

CONTROL-LIABILITY NOTICE

[**Name of Identity Management System**]

Statement of Onus of Control

[state who is in control-whether it is the user or the provider & who makes the decisions]

Statement of Nature of Control

[what users have control over & what they do not have control over]

Rights and Obligations of Users

[short, clear and concise statement/local language based]

Statement of Liability

[user actions/omissions that would incur liability & nature of such liability]

Fig. 1. Control-Liability Notice

4 Conclusion

The user control approach to identity management is not to be disregarded despite the problems it is challenged with. It is a positive approach, but it also has limitations and effects that cannot be pushed to one side in a holistic treatment of the identity management debate. The terminological confusion, the limitations of identity control, privacy and security, the human factors, the fusion of the non-digital and digital worlds and merging of actors must be taken into account.

The most important effect of all is how greater user control in identity management may result in greater user liability. This is why users need all the more to be empowered through awareness of what identity management systems can and cannot do for them and what they themselves will become responsible for. At the moment, this is not very clear to users. The role of academics in responsible dissemination of research information to the general public about identity technologies and systems is the need of the hour. A possible way forward is the control-liability notice, which could be a starting point for further research in the area. Such a notice will enable greater consciousness and make things clear not just for individual users but also for the organisations that implement it.

Acknowledgements

The author wishes to thank all the reviewers who contributed to the shaping of this paper with their valuable comments, suggestions and feedback.

References

1. Bhargav-Spantzely, A., Camenisch, J., Gross, T., Sommer, D.: User centricity: A Taxonomy and Open Issues. In: DIM 2006, Proceedings of the Second ACM Workshop on Digital Identity Management, pp. 1–10 (2006)
2. Cameron, K.: The Seven Laws of Identity, December 5 (2005), `http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf`

3. Sun Microsystems, Identity Management Solutions: Overview, http://www.sun.com/software/products/identity/ (As at January 5, 2009)
4. OpenID.Net, What is OpenID, http://openid.net/what/ (As at January 5, 2009)
5. Higgins: Open Source Identity Framework, The Eclipse Foundation, http://www.eclipse.org/higgins/index.php (As at January 5, 2009)
6. Hansen, M.: Marrying Transparency Tools with User-controlled Identity Management," The Future of Identity in the Information Society. In: Fischer-Hubner, S., Duquenoy, P., Zucatto, A., Martucci, L. (eds.) Proceedings of the 3rd IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School, Karlstad, Sweden, August 2007, pp. 199–222. Springer, Heidelberg (2008)
7. Edwards, L., Brown, I.: Data Control and Social Networking: Irreconcilable Ideas? In: Matwyshyn, A. (ed.) Harboring Data: Information Security, Law and the Corporation. Stanford University Press (2009), http://ssrn.com/abstract=1148732
8. Dhamija, R., Dusseault, L.: The Seven Flaws of Identity Management: Usability and Security Challenges. IEEE Security & Privacy 6(2), 24–29 (2008), http://ieeexplore.ieee.org/iel5/8013/4489835/04489846.pdf?isnumber=4489835&prod=JNL&arnumber=4489846&arnumber=4489846&arSt=24&ared=29&arAuthor=Dhamija%2C+R.%3B+Dusseault%2C+L;
Gotterbarn, D.: Informatics and Professional Responsibility. Science and Engineering Ethics 7.2, 221–230 (2001)
9. Viacom International Inc., v YouTube Inc., YouTube LLC and Google Inc., Case 1:07-cv-02103-LLS, March 13 (2007), http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2007cv02103/302164/1/
10. British Telecommunications plc, Comprehensive Identity Management: Balancing Cost, Risk and Convenience in Identity Management , White Paper, p 7 (2007), http://www.btglobalservices.com/business/global/en/docs/whitepapers/22872_Identity_Mgmt_wp_en.pdf
11. National Computing Centre, Beware fake anti-virus programs, Industry News (Winter 2008), http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_308688
12. Acquisti, A., Grossklags, J.: Privacy and Rationality in Decision Making. IEEE Security & Privacy 3(1), 26–33 (2005)
13. Erasmus, D.: The Praise of Folly, 1514
14. Laurie, B.: OpenID: Phishing Heaven, p. 187, January 19 (2007), http://www.links.org/?; Leyden, J.: How Poor Crypto Housekeeping Left OpenID Open to Abuse, The Register, August 13 (2008)
15. Schneier, B.: Secrets and Lies: Digital Security in a Networked World, p. xi (2000)
16. Eap, T., Hatala, M., Gašević, D.: Enabling User Control with Personal Identity Management. In: 2007 IEEE International Conference on Services Computing, SCC 2007, pp. 60–67 (2007)
17. Joinson, A., Paine, C.: Self-disclosure, privacy and the Internet. In: Joinson, A., et al. (eds.) The Oxford Handbook of Internet Psychology, ch. 16, pp. 237–252 at 248–249. Oxford University Press, Oxford
18. Lyon, D.: Surveillance Studies: An Overview. Polity, Malden (2007)
19. Post, R.: Three Concepts of Privacy. 89 George. L J., 2087 (2001)

20. Heisenberg, D., Fandel, M.-H.: Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard. Paper presented at the Annual Meeting of the American Political Science Association, Boston Marriott Copley Place, Sheraton Boston & Hynes Convention Center, Boston, Massachusetts, August 28 (2002), http://www.allacademic.com/meta/p65517_index.html
21. De Boni, M., Prigmore, M.: Cultural Aspects of Internet Privacy. In: Proceedings of the UKAIS Conference, Leeds (2002), http://www.leedsmet.ac.uk/ies/comp/staff/deboni/papers/Cultural_Aspects_of_Internet_Privacy.pdf; Ruiz, B.: Privacy in Telecommunications: A European and an American Approach, p 40. Martinus Nijhoff Publishers (1997)
22. Privacy International, The 2007 International Privacy Ranking, December 28 (2007), http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597
23. UK House of Commons Home Affairs Committee, A Surveillance Society? Fifth Report of Session 2007-2008, Volume I, Report, together with formal minutes, published on June 8, 2008 by authority of the House of Commons London, The Stationery Office Limited, http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf
24. Wu, T.: Application-Centered Internet Analysis. 85 Va. L. Rev. 1163, 1203–1204 (1999); see also Goldsmith, J., Wu, T.: Who Controls the Internet? Illusions of a Borderless World, p.123 (2006)
25. Ohm, P.: The Myth Of The Superuser: Fear, Risk, And Harm Online, U. of Colorado Law Legal Studies Research Paper, No. 07-14, http://Ssrn.Com/Abstract=967372
26. Sherwin, E.: Infelicitous Sex. Legal Theory 2, 209–231 at p 229 (1996)
27. Westen, P.: Introduction at p 307, and Chapter 8. The Confusions of Consent, 309–336 in The Logic of Consent: The Diversity and Deceptiveness of Consent as a Defense to Criminal Conduct (2004)
28. Samson v Aitchison [1912] AC 844; 82 LJPC 1; 107 LT 106; 28 TLR 559
29. 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
30. Grey, T., et al.: US and EU Authorities Review Privacy Threats on Social Networking Sites: Part 2. ITLT 16 5 (7) (May 1, 2008); Wong, R.: Social Networking: Anybody is a Data Controller!, Working Paper, Revised Version (October 2008), http://ssrn.com/abstract=1271668
31. European Court of Human Rights, Judgment of 6 November 2003, Case C-101/01
32. Metro-Goldwyn-Mayer Studios Inc. v Grokster, Ltd. (04-480) 545 U.S. 913 (2005) 380 F.3d 1154
33. Metro-Goldwyn-Mayer Studios Inc. v Grokster, Ltd., as above
34. EFF, RIAA v. The People: Four Years Later (August 2007), http://w2.eff.org/IP/P2P/riaa_at_four.pdf; Reuters, 459 European P2P users sued, October 7 (2004), http://www.afterdawn.com/news/archive/5675.cfm; J Borland, RIAA sues 261 file swappers, CNET News.com, September 8 (2003), http://news.com.com/2100-1023_3-5072564.html; Engel, J.: Music Industry Targets CMU, The Saginaw News, April 16 (2007) (quoting the RIAA as filing 18,000 lawsuits)
35. The Financial Times Limited v The Blackstone Group LP et al., US District Court Southern District of New York, Case Number 1:2009cv00783, Filed on January 28 (2009)
36. Poppleton v Trustees of the Portsmouth Youth Activities Committee [2008] EWCA Civ 646

37. Cameron, K.: The Seven Laws of Identity, Version 2, August 18 (2008), http://www.identityblog.com/?p=1007
38. R v Spurge [1961] 2 All ER 688
39. Burns v Bidder [1996] 3 All ER 29
40. Privacy Awareness Not Backed up by Behaviour, Survey Finds. Out-Law News, August 13 (2008), http://www.out-law.com/page-9345
41. Council Of Europe, http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Data_Protection_Day_default.asp
42. Opinion on More Harmonised Information Provisions, WP 100, November 25 (2004), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf and Appendices: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100a_en.pdf