# What's Yours is Mine and What's Mine's My Own: Joint Accounts and Digital Identity

***A. A. Adams***
*Centre for Business Information Ethics, Meiji University, Tokyo, Japan*

***S. A. Williams***
*School of Systems Engineering, University of Reading, Reading, UK*

{Digital Identity, Privacy, Security, Social Networking}

## Abstract
Many online services assume that they each account will only be accessed by one person, ever. Thisis even enshrined in the terms and conditions for some. However, our identities are bound up with others in various ways, in both life and death, legally and socially. A basic classification system for multiple ownership of accounts is proposed, based on fictionalised accounts of real world problems encountered by the authors and their acquaintances.

## Introduction
Access to information services is often subject to authentication requirements, many of which correspond to the user asserting an identity, which the system then checks is authorised to access that service. Much of the literature on identity as it relates to digital systems (particularly authentication and access control) discusses only singular users in isolation, and often depends on a strict one-to-one relationship between one user and the segregated part of the system they are permitted to access, and to which no other user is granted access. On the other hand, the Unix operating system has two levels of identity: the userid and the groupid, reflecting the idea that access to some services is limited to a group, not just one individual. In addition, many organisations allow both individual and group userids to be issued for Unix systems. This reflects an acknowledgement that identity is not simply a singular concept of individual people, but that it includes various group elements. In this paper use cases based on real examples are presented in a narrative form, following the concept of Rahaman and Sasse (2010) to define the "lived experience of identity" and show that the current provision for the social and legal concepts of joint identity are currently underdeveloped in information services and need to be address in providing a "human-centric identity system". A new draft classification of types of joint identity is proposed to promote discussion and development in this area in terms of both enhanced terms of service and technical capabilities of information systems and services. This is intended as the start of a broader inclusion of joint identities within identity frameworks and is neither a rigid classification nor a universal solution, but a first approach to a solution of the problem.

Identity is an elusive concept (Jenkins, 2008), with no single clear definition. It is used in many different contexts and for a variety of purposes, ranging from authenticating to a bank to be allowed access to an account, through to our understanding of who we are within a community (Williams, Fleming, Lundqvist and Parslow, 2013). The term is certainly interpreted differently by various academic authors. Goffman (1959) takes the view that self (identity) is constructed by the performance that the individual gives in front of others. While Jenkins (2000) highlights the interplay between: how we identify ourselves, how others identify us, and how we identify them. Camenisch, Lehmann and Neven (2012, p.80) explain it as "we view a user's identity as a set of attributes or, more generally, any information a party knows about a user" going on to discuss the use of these attributes in authentication processes. Buckingham (2008) traces the ambiguous meanings to the Latin root of the term.

Warburton (2010, p.10), through a series of interviews with a group of experts in the area of online identity, identified two extremes that form a Digital Identity continuum:

> "Digital identity can be understood as a continuum. At one end we find the 'simpler' or 'narrow view' where digital identity is 'a collection of credentials online' used in electronic transactions … In contrast, the other end of the spectrum is characterised as the 'fundamental side' or the 'broader view'."

So, identity is multi-faceted. One aspect that has been rather overlooked is that it is often partly joint. This joining together can be a tight coupling of two people, for example a married/co-habiting couple who have a joint mortgage and perhaps other joint bank accounts. It can be an unequal relationship between two or more people, for example a child's email address to which one or both parents maintain access. It can be a broader group, such as a group of friends who go on holiday together or put on plays (the classic amateur dramatic society). Some of these joint identities have legal standing and some do not, and in fact some are legally imposed (biological parents have legal duties to their children in most countries and usually by default some legal authority over them, though either of these may be removed in some circumstances). Some are catered for by some commercial or public authorities, but many are not recognized. As our identities are more and more linked to computational processes for their expression and our actions in the world, the legal and technical affordances offered by third parties for these conceptions of joint identities needs careful scrutiny. When joint identities are not recognized careful balances and expectations of security and trust can be undermined, legal liability can be imposed unfairly and the natural relationships between human beings can be put under pressure by overly rigid algorithmic restrictions designed for the convenience of service providers rather than the reality of human social lives. There are pockets of existing work where consideration is given to issues of joint access for example more than ten years ago the dilemma of keeping medical notes accessible but private was considered (Mandl, Szolovits and Kohane, 2001).

Using a sequence of anecdotes based on real life experiences (of the authors, their contacts or publicly reported cases, although the names and some details have been altered to respect privacy and clarify the issues) various challenges for joint identity in the information age are teased out, followed by an analysis of the trust, security, social and regulatory issues raised, with some suggestions for how service providers and regulations ought to operate. For each narrative, the problem or problems are highlighted and a brief suggestion of improved approaches are given, including highlighting some good, or even best, practice already available from some service providers.

The implications for identity system design and implementation of joint identities are presented using the *laws of identity* proposed by Cameron (2005), suitably expanded upon for our purposes before the draft

classification of types of joint online identity are presented, together with an initial consideration of the solutions they represent but the further problems in security and privacy they might also generate.

# Facebook Addicts

Many students (and others) find that Facebook can be a distraction when there is important work to be done. Ben knew his low scores in last year's exams were partially because he had wiled away many hours reading Facebook when he should have spent the time revising. He knows his self control is limited and so he has hit on the idea of recruiting his girlfriend's help. He will tell her his password and she will log in and change it, then ration his access during the exam period.

## Issues

Ben may be exposing more of himself than he intended to, his girlfriend is now able to access his Facebook account as him:

- Material that he has categorised as not accessible to her (for example the photo of him kissing someone else) she will be able to see.
- She may choose to make some changes to his account that can range from the harmless to the malicious.
- If she inadvertently leaves him logged in in a public place others may access his account.

Lots of other services now offer "login with Facebook" and so he won't be able to access them, while his girlfriend will be able to.

If Ben uses the same password for multiple accounts he may also have given his girlfriend access to his email or even his bank account.

Letting someone else access your account is not within Facebook's terms and conditions and so they may take action against him.

## Alternatives

While the real solution to Ben's issue is learning proper self-control, that may not be possible in time. Providers could consider a double lock that can be applied for a limited time period, allowing a third party to lock the account, but not giving them any other access to the account itself. A time-locking system based on the ideas of bank vaults, which can only be opened even with the keys/combinations during set times, could also be offered, or on the self-limiting systems offered (voluntarily or because of regulation) by many online gambling sites (Nelson et al., 2008), allowing Ben to irrevocably set limits to his own.

# Can I help with your shopping?

Angie is a good neighbour. Fred who lives next door is frail and when the weather is fine Angie drives him to the local supermarket. When the weather is poor he often gives her a list and some money allowing her to do his shopping as well as her own. Fred would prefer to shop online but he is not very confident with using his computer beyond emailing. So he asks Angie if she will set up an account for him and help with placing his weekly order.

## Issues

Fred places a fair amount of trust in Angie when he gives her the money to do his shopping, but the risk is

limited to the amounts he gives her. His risk is much greater with the online shopping as he is effectively giving her access to his bank account. He is also violating the terms and conditions of his bank account and the online shopping service.

### Alternatives

Online shopping providers should consider setting up linked accounts where orders can be prepared by one of a group of trusted friends and relatives, via their own accounts, and the frail shopper only has to be involved in confirming the order, which could perhaps be done by phone or email. A limited set of items might be set by the primary account holder and/or a regular payment limit and restricted delivery address, to prevent abuse of trust.

## What are you reading?

Tim is an avid reader both for pleasure and for his job as a police researcher. He bought one of the first Kindles. His wife Jane reads less and mostly novels so also has a Kindle, and following Amazon's advice they have a shared account. Jane grumbles how difficult it is to find a novel she will like among Tim's plethora of ebooks. In the old days Tim just left recommended books on her desk.

They are thinking of buying a third Kindle for their 12 year-old daughter Maisy. They know she can also share their Amazon account but have several reservations:

- some of Tim's books and the PDFs he has uploaded are not really suitable for a child;
- they are concerned that Amazon's one-click ordering isn't something that Maisy should use;
- looking into the future what will become of this joint account when Maisy becomes an adult?

### Issues

While the Kindle model encourages sharing among families across several devices there are problems that face a family such as Tim has recognised.

- Not all books should be shared;
- One-click buying is settable by anyone with access to the account;
- How can family sharing be made future proof?

### Alternatives

The ebooks metaphor for physical books needs extending, for example families should be able to categorise books as ones that belong to the whole family and those that belong to a subset. In some geographic areas newer Kindle devices do include the facility to offer parents some control over what content their child accesses. Around the world forums for many devices have anxious parents searching for advice on how to use parental controls, or wondering why these controls do not do what the parents had expected, there are some pockets of good practice in providing easy to use "locks", for example in the UK the BBC offer a parental guidance lock. These "locks" are steps that parents welcome but they do not address the nuances of the issues.

## Life after death

Ellie was an only child of only children, when she was young she had travelled a lot with her parents, as an

adult she settled in a new country. Her father and mother divorced and lived on different continents. Ellie was on good terms with both and frequently talked to them using Skype. Her father died unexpectedly, Ellie had to deal with his affairs, which included a traumatic journey to organise the repatriation of his remains.

Eight months after her father's death she was talking to an acquaintance about the problems she had in knowing who her father's friends were and that she knew she hadn't made contact with them all. The acquaintance asked if she had checked her father's email account, Ellie had to admit that she hadn't, but determined that she would, but when she tried she found herself hitting a brick wall.

### Issues

The email provider has no obvious details on their web site as to what to do in the event of death of a user. Their help desk is notorious for sending out robotic replies. When the procedures are discovered they assume the person lived and died in the US and that all the relevant paperwork is both in English and fits with the US procedures. The provider's policy is that after 6 months of no usage on an account it is flagged as inactive and after a further 6 months all data is automatically deleted. They have no allowance for putting these terms into abeyance while formal proof of the death of the primary account holder, and the identity of their executor, is proven.

### Alternatives

Service providers have to appreciate that their users will die and to make appropriate procedures easily findable. They may also need to consider the international nature of life and death. One year may be too short a period to delete all data on an inactive account. some providers are considering issues related to email and death.

There is now a significant community of researchers looking into the issue of death and digital assets (including system accounts). See Edwards and Harbinja (2012) for a recent overview of the legal issues, Carroll and Romano (2011) for discussion on issues of digital legacy, Moncur, Bikker, Kasket and Troyer (2012) for discussion of the role of technology related to the period immediately after death and Viega et al. (2004) for the role digital artefacts play in memorialisation.

## You talking to me?

Dan and Pete have lived together for several years and share most things. They have lots of accounts, and for many of them they have three. For example they both have a Skype account, but they also have a joint one usually logged in when they are at home. They are a couple and many of their friends often just want to speak to either one of them, whichever is available, or want to send an email that either of them can respond to.

### Issues

Does one of them have to be the "responsible" person for each account, or will the provider accept joint responsibility?

### Alternatives

Online service providers could allow for joint accounts in the same way some banks provide them: each person agrees to joint and several liability for the account and has joint access to it. For more control, certain elements of the account (such as changing the password or even deleting contents) might require the consent of both owners.

# Joint Society Account

Nick and Andrea run a small event every year for fans of romance novels in the UK. The UK has no simple way to set up a formal non-profit organisation and the event is too small to justify the costs of running it via a company. Some banks do, however, recognise such organisations and offer a "Treasurer's Account" which allows them to require two signatures on any instruction to the bank. When Nick moved to a different town it became more difficult to deal with the paper-based systems and anyway they both did their personal banking online.

## Issues

Unfortunately the bank has not set up treasurer accounts to allow online access, as they claim they are prevented from doing so by anti-money laundering regulations.

## Alternatives

Should banks be required to allow online banking for all their accounts and not be allowed to hide behind anti-money laundering claims for some types of accounts?

# Junior Emailer

Sam is ten and has an email account at school which only sends/receives internally. One of her close school friends moved away recently and she wants to keep in touch with her by email. Her parents are aware of the dangers of allowing her unrestricted access to the Internet, but don't want her to lose touch with her friend. They set up a Gmail account for Sam, but don't give her the password, she can only log in on the family. Her parents check the account each day and delete all messages except those from allowed senders.

## Issues

They had to enter a false date of birth for Sam to get the account because Google do not allow under-13s on Gmail because of the US COPPA law and their lack of a system in place to verifiably collect such permission of parental/guardian consent.

Currently, email accounts are either "free" (bundled with some other service such as an ISP or paid for with personal data) or technically harder to use.

## Alternatives

Should the law allow a simpler way of registering an under-13s account as an adjunct to an adult account on the same service? The adult account could be set up to automatically act as a firewall for the child account but provide the same benefit to the provider as any other account.

# Analysis of Issues

## International Rescue

The Internet is global and many companies such as Microsoft, Google, Facebook, and Yahoo take great advantage of this to run operations globally from one country (typically the US, less commonly one EU country such as Ireland). Where they do have local operations these still tend to assume that each customer is from the country in which they operate and knows local laws and local languages well. The international nature of some families seems to be often overlooked by even multinational companies. Choice-of-law and -jurisdiction is often part of the terms and conditions of use of an online service (though it is well-known that effectively nobody reads such notifications (Gindin, 2009)). But global companies should surely be

expected to do better in their dealings with global citizens than simply expecting both the citizens and their jurisdictions to follow the norms of the service provider's choice of jurisdiction. Google's "death of account holder" policy for Gmail includes some good practice, but while they accept death certificates in foreign languages with notarised translations they still require a copy of an email sent from the relevant account with all headers attached. The appropriate legal executor may not have such an email and might find it difficult to obtain this information. There are three issues raised here: jurisdiction (including which country's inheritance laws take effect), the property or not status of emails and the property or not status of email and other online accounts.

### Identity Intersections

There are some useful lessons to be learned from the banking sector in dealing well with joint identity concepts, although even here not everything is rosy. In the UK, joint personal accounts between two individuals are common, though limited to only two people. Housing costs are making it increasingly common for unrelated people to share housing in more than just twos. Financial arrangements for two people can be relatively easy, even if they are not related. However, two couples buying a property together end up with only one of each couple being officially on any joint accounts.

In Japan, even two-person joint personal accounts are not available. If a couple wishes to take out a mortgage then they can either split it into appropriate segments and each take out that part (a very complicated process) or one partner can take out the full mortgage. That means, however, that only the partner who holds the mortgage has legal rights to access details and only their income is taken into account in assessing ability to pay. For the first three years of marriage, assets are not yet counted as joint and so partners paying jointly into a mortgage held by only one need to be careful to keep formal records of their separate payments. In the event of the death of one partner within those three years, inheritance does not automatically pass to the spouse (and Japan lacks civil partnerships, although formal "adoption" of an adult is used to provide legal status by some same-sex couples (Maree, 2004)).

The shared Kindle account concept is a modest step forward in acknowledging joint family identity, but a much more nuanced conception is needed in joining accounts together with shared access to some but not all information. The Kindle FreeTime Unlimited allows parents in the US to control the access for young children in the age range 3-8 years old, but does not extend to the challenges with older children.

The aims of laws such as COPPA (Children's Online Privacy Protection Act, 1998) in the US and the Japanese regulations on filtering mobile Internet (Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People, 2008) for young people have appropriate goals. However, the unintended consequences of COPPA have been to force many young people (and their parents) into a choice between no service and subterfuge [i] to obtain services that are seen as a necessity.

Insisting, as many online service providers do, that accounts must be held by individuals and not by groups, runs counter to the reality of families and other social groupings in society. Methods for sharing some accounts, and standard sets of rules for such shared accounts, are definitely needed.

## Proposed Solutions

In this section, we present a basic conceptualisation of the solution space covering many of the problems described in the motivating cases, including an analysis of the risks that these proposals produce, with an analysis of how those risks can be mitigated. This proposal is only a starting point and a general classification of types of account. The specific details of the services offered by an organisation to users

would dictate which of these categories were offered and the exact details of which services would be shared.

## Joint: Several, Shared, Subordinate, Nominees

We propose four broad categories of shared identities. The first is the *several* account where multiple individual identities jointly own an additional shared account over which they all have complete authority. *Shared* accounts are similar, but include mechanisms for privileging some members of the group over others, in the matter of adding extra members to the group for example. *Subordinate* accounts allow one party to grant specific limited access to one or more other parties. *Nominee* accounts allow for the selection of one or more users to be granted some access or control over an account depending on certain circumstances being demonstrated, such as the death or long-term incapacity of the primary account holder. These capabilities embody the principles of the *Laws of Identity* proposed by Cameron (2005), but instead of the focus being on single users and service providers as they are usually interpreted, they include service providers and multiple users:

1. User Control and Consent: users should have the power to share their accounts with other users based on appropriate consent and not be forbidden by terms and conditions to share service access, which gives rise to an all-or-nothing concept of sharing, as demonstrated in the *Facebook Addicts narrative*.

2. Minimal Disclosure for a Constrained Use: users should have the power to include other users in the set of those to whom it is acceptable to disclose some information. Families should be able to share some of their Kindle content with other family members without giving them access to everything, as shown in the *What are you reading?* and *Junior Emailer* narratives

3. Justifiable Parties: users should have access to the authentication system of the service provider to safely share elements of the service with at least as much certainty of security as their own authentication provides to others, to deal with the situations shown in the *Can I help with your shopping* and *You talking to me?* narratives. The work of Brands (2004) on privacy-preserving identity management can be applied here where instead of sharing limited information with one's medic, one instead shares limited elements of one's accesses with another user.

4. Directed Identity: instead of considering identity to be directed only between service provider and service user, we must consider the broader set of directionalities that are appropriate, not just uni-directional and omni-directional as Cameron suggests, but selectively directional and context-dependent. This idea underlies all of the narratives.

5. Pluralism of Operators and Technologies: again, Cameron's conception is good, but does not go far enough in recognising the social construction of our identities and the need for this pluralism to account for user-user interaction mediated by the provider.

6. Human Integration: again, the presentation by Cameron (2005) is limited to a view of one user and multiple providers and it needs expanding to multiple users interacting with the same and different systems in ways both joint and individual.

7. Consistent Experience Across Contexts: the identity choices given by Cameron require expanding to allow multiple joint identity concepts as well as multiple individual concepts.

*Several* accounts are the easiest concept to institute. Such accounts are simply an intersection of individuals,

where each individual has complete authority over the joint account. The benefits to the service provider of adding these is that they are providing a service that their customers are already providing for themselves by violations of terms of service (usually simply by sharing credentials). By enabling individual logins to share joint accounts, the separate identities of those sharing are known to the service provider. By offering such a service, the provider gains more information (usually the currency in which they are paid) about the relationships between customers. In addition, each individual customer then has their own separate account, providing an opportunity for encouraging all users of a joint account to use the service individually as well as jointly. At present those using joint accounts may well deliberately avoid that service for their individual use because of the common difficulty of multiple accounts with one provider.

*Shared* accounts provide more security for the members of a group against bad actors within their group. Access to information about the account is available to all members. However, some or all other operations may be set to require permission from multiple members of the group, perhaps even specific sub-groups. Consider a small society financial account. All members might be given the right to read and download the financial statements of the group, encouraging transparency about the group's finances. Adding new members to the group might be restricted to a set of people (committee). Making payments might require the authority of the chair and one other. Changing the person fulfilling committee roles might be set to require approval of all or almost all of the committee, or even of a majority of the members of the community.

*Subordinate* accounts are envisaged as primarily useful for parents to provide accounts for their children, or for other guardians of the legally less than fully competent, thus allowing those people to participate in the information society while a known fully competent member of society provides authority and accountability. The supervisory member does not necessarily need to be provided with complete control over the subordinate account. For an email account, for example, the supervisor's access might be limited to seeing the addresses of incoming and outgoing messages, but not their contents. They might have authority to restrict the account to sending/receiving messages to/from only a whitelist, or may act as a human filter system on incoming messages, but have no authority over outgoing messages. Simple emails might be invisible to the supervisor, but attachments could require their approval. Multiple supervisors could be allowed, to take into account both parents overseeing their child's email and sharing the burden of oversight. Such accounts might also be useful for the "shopping help" scenario presented above. The intended customer might work with a staff member of the retailer to create their account and provide limited access to a helper, such as preventing changes to or addition of delivery addresses, placing limits on what might be bought or how much might be spent in one week or month. While unnecessary for most non-abusive relationships, these approaches could provide easy ways to build trust between parties in analogous ways to existing real world approaches.

Many people make Wills that direct what they wish to happen to their possessions after their deaths and in England a Lasting Power of Attorney (formerly Enduring Power of Attorney) allows nomination of someone to make decisions about another's welfare, money or property, when they no longer wish or no longer have the mental capacity to do so (other jurisdictions frequently have equivalent legal instruments). Those without the foresight to make such arrangements are covered by whatever local regulations dictate. Use of nominees would provide a system whereby primary users might set up provisional access to their accounts based on certain circumstances, particularly infirmity or death. A simple set of rules should be developed that would allow for dealing with digital assets which are scattered around the world alongside physical assets. So, for example, an account which is not accessed for six months might be set to allow access to one or more family members instead of being automatically marked for deletion. A nominee

might simply be given the authority to keep an account "live" without actually being able to access it, allowing time for legal processes to take their course, or just for the nominee to deal with all the affairs of a deceased relative over time, instead of placing a relatively short time limit on such systems, at a time when people are often very distressed.

## Entailed Risks

Joint bank accounts in the UK present a risk of betrayal by one of the account owners and legally these are regarded as jointly held assets. So, flatmates with a joint account set up to receive payments from both parties to cover bills might be "plundered" by either party for other purposes. Any joint identity account will require some level of trust between the parties. Where people have some joint affairs, inter-personal pressure may in some cases lead to the adoption of overly trusting or dependent situations. However, the lack of suitable options at present is generating far worse risks alongside violations of terms and conditions.

Subordinate accounts fall into two broad categories: accounts for children and accounts for adults with limitations. Child accounts must grow with the child and within a set of guidelines, the child should be allowed greater access to and control over the account as they age. The parent should similarly have less control and access. At the local age of majority such accounts should automatically be transformed into sole accounts held by the child. Many organisations at present do not even seem to consider the passage of time and maintain age restrictions in perpetuity suitable to the age of a child when they joined.

Limited accounts for adults are more problematic as they represent a broader range of circumstances. An adult with learning disabilities, for example, may or may not progress in capabilities as they grow older. Older adults in general will see only a decline in their situation, but there may be ebbs and flows in their condition. In cases such as assisted shopping, the issue may well be primarily one of familiarity with technology and so there the dependency may reduce over time. A clear and relatively broad set of options needs to be defined for such accounts and appropriate external social and legal safeguards needs to be put in place. Penalties for the misuse of such joint accounts should perhaps be defined in law and protections against the abusive creation of such arrangements need to be instituted.

Arrangements for the transfer of subordinate account holder(s) must also be put in place: it is a sad fact that carers do not always outlive those they care for. Care will also be needed at the time of death of any primary account holder as the secondary may no longer have any legal entitlement to access the account. Service providers need to consider multi-lingual issues when offering services worldwide. While users may be competent enough in a language in which providers offer their services, formal documents such as wills and death certificates will most often be in national languages and service providers may well be caught between the costs of translation and legal advice in that jurisdiction or the risk of continuing to allow access by unauthorised parties.

*Prof Andrew A. Adams is Professor of Information Ethics at the Graduate School of Business Administration and Deputy Director of the Centre or Business Information Ethics at Meiji University in Tokyo, Japan.*
*(e-mail: aaa@meiji.ac.jp)*

*Prof Shirley Williams is Professor of Learning Technologies at the School of Systems Engineering at the University of Reading, Reading, UK.*
*(e-mail: shirley.williams@reading.ac.uk)*

# Conclusions

"No man is an island" and everyone's identity is bound up with others in their life. Sometimes that binding is tight enough that joint agency in the world is a useful or even necessary concept. As our agency in

the world becomes more and more connected to our identity in the online world, the online world must have its ability to handle joint identity improved. Without this, security, privacy, adherence to reasonable conditions of use, accountability for actions and other desirable features of the online world, are seriously degraded.

## References


Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People (Act No. 79 of 2008, Japan).

Brands, S. (2004). Non Intrusive Cross-Domain Identity Management. In 3rd Annual PKI R&D Workshop (Keynote Address), http://middleware.internet2.edu/pki04/proceedings/cross_domain_identity.pdf (accessed 28 June 2013).

Buckingham, D. (2008), "Introducing Identity", in Buckingham, D. (Ed.) Youth, Identity, and Digital Media, The MIT Press, Cambridge, MA, pp. 1-24.

Camenisch, J., Lehmann, A. and Neven, G. (2012), "Electronic Identities Need Private Credentials", IEEE Security & Privacy, Vol. 10, pp. 80-83.

Cameron, K. (2005), "The laws of identity", available at http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (accessed 28 June 2013).

Carroll, E. and Romano, J. (2011), Your Digital Afterlife, New Riders, San Francisco.

Children's Online Privacy Protection Act of 1998 (codified in US Code Title 13, sections 1301-8).

Edwards, L. and Harbinja, E. (2013), "What Happens to my Facebook Profile when I die?': Legal Issues Around Transmission of Digital Assets on Death", Working Paper No. 5, CREATe, University of Glasgow, Glasgow. http://www.create.ac.uk/what-happens-to-my-facebook-profile-when-i-die-legal-issues-around-transmission-of-digital-assets-on-death (accessed 28 June 2013).

Gindin, S. E. (2009), Nobody Reads Your Privacy Policy or Online Contract: Lessons Learned and Questions Raised by the FTC's Action against Sears. NorthWestern Journal of Technology & Intellectual Property, 8(1), 1-37.

Goffman, E. (1959) The Presentation of Self in Everyday Life: Penguin, London.

Jenkins, R. (2000), "Categorization: Identity, Social Process and Epistemology", Current Sociology, Vol. 48 No. 3, pp. 7-25.

Jenkins, R. (2008) Social Identity (Key Ideas), Third ed. Routledge, London.

Mandl, K. D., Szolovits, P. and Kohane, I. S. (2001), "Public standards and patients' control: how to keep electronic medical records accessible but private", BMJ, Vol. 322, pp. 283-287. http://dx.doi.org/10.1136/bmj.322.7281.283 (accessed 28 June 2013).

Maree, C. (2004) "Same-Sex Partnerships in Japan: Bypasses and Other Alternatives," Women's Studies, Vol. 33 No. 4, pp. 541-549.

Moncur, W. , Bikker, J., Kasket, E. and Troyer, J. (2012), "From death to final disposition: roles of technology in the post-mortem interval", in Konstan, J., Chi, E. H. and Höök, K., CHI '12: Proceedings

of the SIGCHI Conference on Human Factors in Computing Systems, ACM, New York, NY, pp. 531-540.

Nelson, S. E., LaPlante, D. A., Peller, A. J., Schumann, A., LaBrie, R. A. and Shaffer, H. J. (2008) "Real limits in the virtual world: self-limiting behavior of Internet gamblers", Journal Gambling Studies, Vol. 24 No. 4, pp. 463-77.

Rahaman, A., and Sasse, M. A. (2010), "A framework for the lived experience of identity", Identity in the Information Society, Vol. 3 No. 3, pp. 605-638.

Viégas, F. B., boyd, d., Nguyen, D. H., Potter, J. and Donath, J. "Digital artifacts for remembering and storytelling: posthistory and social network fragments," in System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on, p. 10-19. http://dx.doi.org/10.1109/HICSS.2004.1265287 (accessed 28 June 2013).

Williams, S., Fleming, S., Lundqvist, K. and Parslow, P. (2013), "This Is Me: Digital Identity and Reputation on the Internet", in Warburton, S. and Hatzipanagos S. (Eds.), Digital Identities and Social Media, IGI Global, London, pp. 104-117.

Warburton, S. (2010) Digital Identity Matters, King's College London, London. http://digitaldisruptions.org/rhizome/wp-content/uploads/2010/06/rhiz08_DigitalIdentityMatters.pdf (accessed 28 June 2013).

[i] http://productforums.google.com/d/topic/gmail/NZYEBW3Nd_o (accessed 28 June 2013).