Security and Privacy Considerations in Digital Death

Michael E. Locasto
University of Calgary

Mike Massimi
University of Toronto

Peter J. DePasquale
The College of New Jersey

ABSTRACT

Death is an uncomfortable subject for many people, and digital systems are rarely designed to deal with this event. In particular, the wide array of existing digital authentication infrastructure rarely deals with gracefully retiring credentials in a uniform fashion.

This research paper highlights an emerging paradigm: gracefully dealing with expired digital identities in a secure, privacy-preserving fashion. It examines the confluence of modern browser technology, cloud services, and human factors involved in managing a person's digital footprint while they live and retiring it when they die.

We contemplate a potential approach to dealing with credentials after death by using cloud computing. We consider the reasons that such an approach may actually provide an opportunity for enhancing authentication security by frustrating identity stealing attacks.

We note that this paper is not aimed at trivializing the real grief and loss that people feel, but rather an attempt to understand how security and privacy concerns are shaped by the end of life, with the ultimate goal of easing this transition for friends and family.

Categories and Subject Descriptors

H.1.1 [**Models and Principles**]: Systems and Information Theory—*Value of Information*

General Terms

Security, Measurement

Keywords

digital end-of-life, death, identity containers, cloud identity management

1. INTRODUCTION

This paper considers the security and privacy issues involved in the management of digital identities during and at the end of life, and whether a technological solution exists that can ease management and increase assurance against digital identity theft.

NSPW'11, September 12–15, 2011, Marin County, CA, USA.

The focus of this paper is on identifying what kind of changes in authentication technology might more easily support security and privacy goals in passing on control of critical online identity aspects. In short, how do we apply *thanatosensitive design* (see Section 6) to information security?

1.1 Digital Footprints

Death can be an unpleasant subject. Yet, as we get deeper into the digital age, each of us leaves behind an even greater digital identity footprint, and managing the retirement of that collection of digital identities is an important task that falls on family members and friends after someone dies. Both practical and emotional issues abound: how do I close this online bank account? Should I leave up their hobby Web page or Twitter account [5] as a tribute to their passion? What do I do with 7GB of their email?

We accumulate a startling about of digital debris, and this statement seems particularly true of those born from 1990 onward, as we can see with the surge in social networking and increasingly visible online lives. The digital information age is young enough that most participants are only beginning to deal with the management of digital identity and privacy concerns when loved ones die. Our digital footprints go far beyond embarrassing Facebook images. The transformation extends to the economy, society, and government: social networking, e-commerce, and "digital government" delivery systems are where our banking, retirement accounts, travel, shopping habits, book reading, music preferences, food ordering, etc. all take place online.

At the same time, most of our current identity management infrastructure is rife with problems as old as low-entropy, guessable passwords or password reuse across accounts. The HBGary Federal saga reminds us that both weak passwords and password reuse across accounts is still rampant [2]. Clearly, there is a need for strong management of multiple *independent* digital identities (in essence, containers: see Section 4).

1.2 Personal Identity Retirement, Revocation, and Cleanup

Personal digital identity and credential systems are typically set up with little thought as to how credentials might gracefully be retired *in conjunction with other aspects of your digital identity*. Even retiring individual credentials for organizations and machines is a known hard problem: for example, although mechanisms exist for certificate revocation, its use is subject to substantial challenges (e.g., cache coherency, certificate revocation list size and update frequency) in many environments.

For the retirement of *personal* identity information, the problem becomes somewhat more delicate. We note that our definition of "cleanup" goes beyond just deleting the account and content. Most

individual authentication mechanisms seem to assume a worldview in which they are the only extant mechanism, and "unsubscribing" or deleting an account is as simple an action as logging in, navigating to a settings or profile management page, and asking the site to permanently disable or delete the account.

This paper suggests that the paradigm of holistic digital identity management is more complex than that assumed by any single authentication mechanism or Web site account.

1.3 Our Definition of Identity

When we say "*identity*", we mean the collection of information about a user contained in services as varied as banking and social networking. Such information includes both server and user-generated content and data.

We see identity as including (1) *credentials* (i.e., usernames, passwords, passphrases, email addresses, public keys, certificates, identifiers, roles, password "hint" questions and answers, SiteKey phrases and pictures) used to authenticate to the service and authorize different uses, (2) *user preferences* for interacting with that online identity, (3) *personal information* (i.e., names, account numbers, address, contact information, date of birth, sex) stored by the service, and (4) *content* (e.g., account balances, comments, links, likes, posts, medical ailments) generated during the interaction of the user with the service.

We stress that this definition is not a complete one (although the "content" component is meant to cover most data not contained by the other three identity components we specified), but rather a reasonable working definition of the major types of data related to an individual's real identity that they may wish to control.

1.4 Motivation: Containing ID Breaches

Our motivation to examine the possibility of well-managed end-of-life digital footprint erasure or retirement stems from recent incidents highlighting the very old problem of poor quality, reused credentials in software systems ranging from desktops to web sites.

We were motivated to explore this topic by thinking about classic problems with password-based authentication that are particularly compounded in an age where the demand for login credentials from multiple Web sites and services increases the pressure on ordinary end users to take shortcuts, including weak passwords and password reuse across multiple sites.

From a systems perspective, these identities are not compartmentalized. Given the expediency of using weak passwords and the existence of security-weakening measures like password recovery questions, guessing, brute-forcing, or deducing login credentials is relatively easy. Furthermore, given the prevalence of password reuse, corrupting even a single low-importance account holds the potential for corrupting a larger slice of someone's digital identity.

Although identity management systems like OpenID exist for making it easier and more secure (by reducing the proliferation of weak authentication schemes and "roll your own" crypto, or so the claim goes) to log in to multiple web sites, web applications, and software, OpenID faces its own set of challenges and still supplies a single point of identity failure; a compromise of the main OpenID account leaves a large part of your digital identity open to access and manipulation.

What seems needed, then, is a system for creating identity containers that (1) use strong credentials like completely random passwords, (2) are strongly isolated from one another (i.e., a compromise of one set of credentials does not directly lead to a compromise of even a single other digital identity component), and (3) does so in a fashion largely transparent to the end user (in other words, a user has no chance to create a weak password or reuse a password because they are removed from these decisions).

Assuming that such a software system and service could be built (we sketch a design in Section 4) and done so in a way that is usable and transparent, we next thought of the implications the deployment of such a service would have. For example, centralizing the management of all your online identity "aspects" opens up the possibility of greater control and greater abuse. But perhaps more fundamentally, given that our online digital identities are likely to grow by accretion as larger segments of society in the developed world move online, it is natural to ask: what happens to all this accumulated information when we die? What are the design considerations for our identity authentication mechanisms such a system might interact with in the eventuality of death? In other words: how do we design authentication mechanisms that explicitly provision a mechanism for dealing with the death of the account holder and passing control to a designated beneficiary (or set of beneficiaries)?

1.5 Contribution

This paper attempts to examine the issues involved with the *multi-lifespan* management of digital identity. It examines the paradigm of how to contend with authentication and credential management of a single real person after their death. The key challenge is to gracefully deal with expired digital identities in a secure, privacy-preserving fashion. We examine the confluence of modern browser technology, cloud services, and human factors involved in managing a person's digital footprint while they live and retiring it when they die. We pay particular attention to the design of an authentication and identity management infrastructure aimed at containing identity theft to a particular "identity container" stored in the cloud.

Proactive deletion of information carries a cost. Traditional authentication technologies present roadblocks to coherently and cleanly retiring a digital footprint in a single fell swoop. How can we better manage authentication credentials from the point of view of preparing for the event of death?

1.6 Assumptions

We make several assumptions that not all might agree with. First, it is a desirable goal to ease the management of the decisions that the bereaved must confront. Second, account holders wish to pass on parts of their digital identity to a variety of survivors. Third, although deaths are significantly less frequent relative to "common" authentication actions like logins, they are of sufficient importance so that the mechanism should deal gracefully with matters of transferability. Finally, we leave open the question of how to encourage people to undertake planning; we note that people delay other related concerns like retirement planning and life insurance. We believe that those concerned enough with their digital legacy would like some kind of unified management of their digital identity, and we suggest that increasing amounts of modern life will transition to the digital arena, making the task of retiring a digital identity more common or needed than traditional physical interactions like visiting a brick-and-mortar bank to close an account – particularly due to scalability issues in terms of the relative amount of physical vs. virtual interactions people are likely to have.

2. DIGITAL IDENTITY FOOTPRINT

How large are our digital footprints?[1] As an anecdotal approach to answering the question, one of the authors has over 300 entries in

[1]Answering this question in a more scientific fashion, via a broad survey of a variety of users, is one of our intended follow-on research activities.

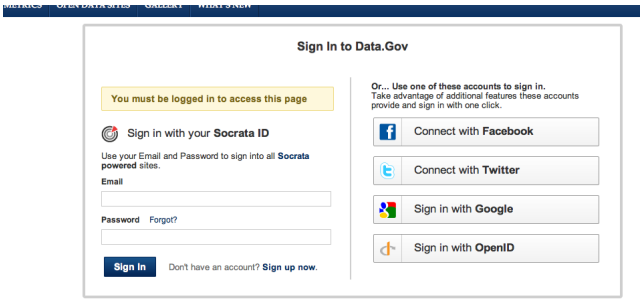


Figure 1: *Accessing Open Government Data Requires Authentication*. As the ease of supplying "login"-like authentication proliferates, sites have decreasing incentives to not include them, and this supplier of `data.gov` seems to require a login for certain information (in this case, a link to the list of data centers that the US Federal government plans to close). This "login" requirement seems troubling, particularly for a government effort that is billed as transparent and open. (Maybe it stems from the provider's need to track and report on its own value as a Federal contractor — but this is pure conjecture on our part).

a password database containing credentials for multiple Web sites, devices, and machine accounts. We suspect that many users can own to significant numbers of accounts and credentials, each forming a part of their total online identity.

Furthermore, it is likely that our digital identities will only grow more complex. As new services come online, and early adopters and the general public create accounts, these services may wane in popularity (see, e.g., MySpace). People are therefore likely to accrue accounts (for example, MySpace to Facebook to Google+). There is little incentive to proactively delete old accounts and email addresses; users simply "move on." Second, as institutions like the Federal Government start to require online interaction (and institutions like banks make it more attractive by charging fees for in-person services), large segments of the population will have no choice *but* to move to some form of online interaction. Figure 1 shows how data.gov requires a form of authentication in order to access some data. Setting aside privacy concerns, this type of interaction is likely to become more common for otherwise innocuous reasons like tracking the value of the contractor or the popularity of certain content. In some sense, because online authentication has become easy enough to deploy as a service, there is little incentive **not** to employ it, but such practices only increase the complexity of dealing with retiring multiple digital identities.

These online accounts naturally have varying importance. A community newsletter may have less relative importance than an account with the Bank of Montreal (BMO). And these accounts may have varying levels of importance in the time following our death. The bereaved will certainly have to dispose of virtual (e.g., frequent flyer miles, fantasy baseball rankings), physical, and financial assets, but may also have emotional needs to satisfy by more deeply analyzing the digital aspects of a loved one's identity. Yet, wading through all these accounts (or even gaining access to the machine where the bulk of credential information is stored) may be a large technological hurdle for most people.

Our kin and executors have an interest in and important responsibility to dispose of our financial assets, but these may be scattered across multiple banks, financial institutions, and credit companies, all of which have an increasing online presence and a diminishing brick-and-mortar presence. They may have to work with our online tax preparer, multiple retirement accounts, multiple banks (possibly in multiple countries), and several credit card companies. Estate management by our family and executors is no easy task, and the amount of digital interaction and access through an inaccessible set of credentials only makes the task more daunting.

Our family and friends may have an interest in our online social circle (and we may have an equally strong interest in preventing them from discovering it); those in it (e.g., Facebook, LinkedIn, Twitter) may wish to learn about our passing.

Our professional circle (professional organizations like ACM or IEEE, our colleagues, research partners, funding agencies, students, scientists) also has an interest in learning about one's passing and possibly obtaining access to research material, code, reports, articles, and other intellectual property.

It seems, then, that most of our online lives will need to be disposed of in some way, but existing authentication frameworks don't make this an easy task. Furthermore, we should have the ability to control such dissemination in a fine-grained fashion; one should be able to specify which sites, accounts, and identity aspects are available or accessible to which type of "identity beneficiery."

2.1 Value of a Unified Approach

A unified approach to digital identity retiring and cleanup offers control to both the bereaved and the deceased. Our family members are likely to only think of financial and work benefits issues in the short term. In time, they will likely want or need access to a larger piece of the decedent's digital identity. A unified framework for identity management could provide quicker access (vs. going through legal channels), and it could help the bereaved bypass the types of restrictions that we see in the Yahoo terms of service imposed on accounts of the deceased. Such an automated mechanism would also relieve service providers of the burden of verifying death certificates or retrieving backups of deleted data for persistent kin. It also offers a degree of control to us while we are alive: we can specify which people will have post-mortem access to specific files and data. Such a facility could be particularly helpful in awkward situations (hidden bank accounts, etc.).

2.2 ID Management

Today, we may depend on a privately stored file, a paper folded in our wallet, or our browser to store the URL, username string, and password required for entry into these sites. We may reuse a single contact email across accounts and even use (and reuse) a weak password. Password recovery hints (or links) for many sites are sent to our contact email account. All these factors make it easy for attackers to hijack a significant part of our digital presence by compromising only a single set of credentials.

3. SURVEY OF TERMS OF SERVICE POLICIES

Revoking single, purely digital credentials such as X.509 certificates is a known hard problem. Gracefully retiring *personal* identity information poses a somewhat more difficult problem. In fact, some Terms of Service contain provisions that make such cleanup difficult, even for those that survive the account holder.

While some services (notably Amazon[2]) neglect to specify how accounts should be terminated, other services do sometimes con-

[2]`http://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088`

Inactive Accounts/Account Closing	
After two year notice of inactivity.	$20.00
After three years of inactivity.	$20.00
After four years of inactivity.	$20.00
After five year notice of inactivity.	$30.00
After six years of inactivity.	$30.00
After seven years of inactivity.	$30.00
After eight years of inactivity.	$30.00
Nine year notice of transfer to Bank of Canada. The nine year notice of transfer to the Bank of Canada does not apply to U.S. dollar and Euro accounts.	$40.00

Figure 2: *Scotiabank*. Scotiabank charges an account for inactivity, and has a nine-year horizon for transfering the account to the care of the Bank of Canada.

template death within their terms of use. For example, the Yahoo terms of service[3] state:

> **No Right of Survivorship and Non-Transferability.** You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted.

Even when thought is given to handling the retirement of an account, its usability seems quite low. For example, email accounts might be set to expire after a year or so of inactivity. The Yahoo YMail Terms of Service state that an account may be suspended for a variety of reasons, including *"...(e) extended periods of inactivity,..."*, and that the actual enactment of such a suspension may take one of several forms:

> (a) removal of access to all or part of the offerings within the Yahoo! Services, (b) deletion of your password and all related information, files and content associated with or inside your account (or any part thereof), and (c) barring of further use of all or part of the Yahoo! Services.

Such terms of service seem to provide little in the way of comfort or usability for those mourning the loss of a loved one.

3.1 Overview of Policies

We examined policies for several types of accounts (Banking, Social, Healthcare, Cloud Services, and Email) across the United States, Canada, and the UK. This study is still ongoing; we present our partial results in Table 1 and anticipate having more by the workshop.

Some reviewers asked us to take a more international view on this topic; we are in the process of gathering data for multiple countries (primarily English-speaking, e.g., US, UK, Canada, Australia). In Table 1, there are a few things to note. USAA does not have a death or transfer clause, but states that certain provisions will remain in force past the Agreement termination. Wells Fargo's online account terms of service only talks about death in reference to terminating a "Delegates" access (a Delegate is defined as someone with temporary legal control of the account).

English-speaking Canada does not have separate Facebook domain (instead it uses facebook.com). Google Health (which is winding down) does not provide any survivorship clauses in the Google Health TOS, Google Health Privacy Policy, or the Google Account TOS. We plan to expand the E-health category with TOS from E-health agreements of Canadian Provinces and US States.

We note that most services contain language about the user's responsibility not to share login credentials or let others use the account. Very few talk explicitely about death, the bereaved, or executors; of the ones that do (such as Yahoo!) they typically forbid such transfer.

[3] `http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html`

4. CLOUD IDENTITY CONTAINERS

In this section, we sketch the design of a system meant to manage multiple independent aspects of our online digital identities. A side effect of our attempt to consider the trustworthiness properties of such a digital identity management "solution" is to consider how this framework might be used in the event of the identity-holder's death.

4.1 Observations

Users already trust their web browsers to store a collection of usernames and passwords for a variety of different Web sites; one author has nearly 180 entries representing over 100 Web sites in one of his frequently-used browsers, another has about 85, and the third has 15.

Users should not have to invent or create strong password material. A trusted agent (such as a browser extension) running locally can do this task. This includes answers to things like "password hint" questions. Some browser extensions (and Apple's Airport Utility) already provide such a "strong password" creation service. More generally, users should have the burden of of managing and remembering credentials removed from them.

Aspects of a user's digital identity should be strongly separated from other aspects. For example, a user's Amazon cloud services account should not share an email address, username, or password with a photo sharing Web site. An attacker that manages to learn the Amazon credentials should not be able to access the photo sharing Web site and vice versa. In essence, an identity management solution should provide "identity containers" that are strongly isolated from each other.

Storing credentials and other account information locally on disk or semi-persistently in the browser's memory is less trustworthy than storing them in a special purpose, remote access facility.

Remote management of identity credentials offers users the ability to bypass restrictions like deletion of their personal information should they die or be otherwise unable to access the data.

4.2 Design

We envision a browser extension that augments current "password management" browser (and extension) functionality. Such a browser extension would:

1. intercept the process of creating credentials for each new Web site or Web application
2. ignore (but record) passwords supplied by the user
3. generate a strong random password
4. generate strong random "password hint" questions and answers
5. create a new, disposable single-purpose [11] email address and other digital identity aspects (e.g., Facebook, Twitter, LinkedIn, blog, Amazon account, eBay account, Skype account)

Category	Country / Service	Death/Transfer Clause ?
Email		
	USA	
	Gmail	No
	Hotmail	No
	Yahoo Email	Yes
	UK	
	Gmail	No
	Hotmail	No
	Yahoo Email	Yes
	Canada	
	Gmail	No
	Hotmail	No
	Yahoo Email	Yes
Social		
	USA	
	Facebook	No
	Google+	No
	LinkedIn	No
	UK	
	Facebook	No
	Google+	No
	LinkedIn	No
	Canada	
	Facebook	N/A (US)
	Google+	No
	LinkedIn	No
E-Health		
	USA	
	MS HealthVault	Yes
	Google Health	No
Banking		
	USA	
	USAA	No*
	Bank of America	No
	Wells Fargo	Yes*
	Citibank	Yes
	Canada	
	Scotiabank	No
Cloud Services		
	USA	
	Amazon	No
	Google	Yes
	Microsoft	No

Table 1: ***An Overview of Various Terms of Service Relating to Account Transfer or Death*****. Most Terms of Service Agreements have language or a clause stating that the account holder agrees to keep their login credentials "secure and confidential" and not to permit others to use the account. Most do not have a clause that deals with transfer of control due to death; a few mention "successors" or "survivors." Policies differ even within a company.**

6. pass through any CAPTCHA-style queries involved in creating these new digital identity aspects to the user via the browser interface

7. store this digital identity information in a cloud storage service

8. retrieve this information when the browser attempts to log into a web site due to user action

One criticism here is that we still need to authenticate the fact that a user initiated a log-in to a particular website, and that relying on the user to supply weak credentials essentially protects high-value credentials with low-value credentials. We are open to suggestions about a more secure mechanism.

4.3 Cloud Storage

Rather than storing credentials locally where they may be subject to theft by malware, the extension can forward them to a cloud storage service; this service essentially becomes a trusted identity container provider. This provider can encrypt and distribute these identity containers in ways that make it difficult for an attacker to subvert or steal multiple credentials at once. Furthermore, since the browser extension creates individual profiles and contact information (e.g., email address) for each credential, an attacker that gains control of a single credential or email address (for example, via disclosure by the email provider) will only have access to that particular identity information. This type of service is particularly useful to survivors that do not have local access to the decedent.

Why Cloud?.

One observation we received in early reviews of this paper was the question: "why is cloud computing involved here?" We mention the use of cloud computing not in an effort to jump on some hype-fed bandwagon, but rather as a reasonable, modern platform for delivering an identity management service to end-users. Our focus on cloud is mainly to help focus the shape of an independent identity inheritance / management service along concrete lines. What is important about this service is the business model, and the collection of technologies and techniques behind what might be currently termed "cloud computing" provides a relatively low barrier to entry for those wishing to provide such a service. In some respects, projects like KeePass that can store their password database in Dropbox are early versions of such a service, but lack the management and inheritance components we discuss below. In any event, the specific technology is less of a focus; we suggest browser extensions and cloud storage only a means to show how such a service may practically be deployed with current technology.

4.4 Handling Identity Inheritance

The user should have the ability to arrange with the cloud provider which set of identity containers is revealed to which set of survivors. In other words, the user specifies which aspects of their digital identity are forwarded to which "identity beneficiary" upon their death.

The user can also choose what combination of events might trigger a transfer of identity information; certain containers may be released if the user fails to respond to a keepalive test (e.g., something like deathswitch.com or a semi-annual email reply requiring a human rather than automated answer), and certain other containers may be released only on presentation of a death certificate and other identifying information.

The identity container provider could also offer to save (independent of the functionality of a specific identity container) other critical physical or virtual documents (e.g., SSN card, birth certificate, legal or financial documents) to be delivered with control of the container to the survivors.

4.5 Service Partners

One substantial obstacle to such a system is the required "network effect" of getting multiple Web sites to buy-in to allowing their users to use this service.

While the service *could* be deployed without the permission of the Web sites that the user interacts with, the user might be violating the Web site terms of service by allowing others to access the account after they have passed.

As a practical matter, getting broad acceptance for such a service will likely be made easier by gaining the cooperation of various service providers; they should be persuaded to include exceptions for such services in their conditions of use and terms of service. Sites would have to "buy in" to the service. One way they may be convinced to do so is that users might be attracted to their services if users know that the services are certified or compatible with transfers of ownership in the event of death. Furthermore, these service providers (e.g., Google, Amazon, Microsoft) face a scalability problem: it may pose significant workflow problems to have to manually respond to everyone with a death certificate seeking access to a loved one's data. Handing off this service to a trusted third party may provide an attractive solution.

Another obstacle is the economic model for this service. It would be too close to extortion to ask survivors to pay a fee for access to someone's data; a subscription model, where the cost is borne by the user while they are alive (similar to a life insurance model) seems much more workable. Still, the identity container provider faces *significant* risks from external attacks because it is a publicly known source of credential information. A serious compromise could lead to multiple identities being disclosed, and the potential for an insider attack might be significant. These pressures might increase the cost of protecting such a service far beyond what people might be willing to pay.

Furthermore, although large organizations like credit rating agencies might have the financial resources to take on such a service, they may have a conflict of interest in administrating this information, and are likely to view it as part of their intellectual property, rather than seeing their role as a trustee of sensitive third-party information.

5. DISCUSSION

One of the best ways to avoid information disclosure is *not to store data in the first place*, but such restraint is not common, and proactive deletion of information carries a real cost (time and energy spent to trace information and securely erase it). Traditional authentication technologies present roadblocks to coherently and cleanly retiring a digital footprint in a single fell swoop. How can we better manage authentication credentials from the point of view of preparing for the event of death?

We wish to facilitate discussion at the workshop on the following questions:

1. *Is it possible to design even a single authentication mechanism that gracefully handles the event of death?* Setting aside the question of how to federate or manage multiple identities, can a single authentication mechanism gracefully expire credentials or automatically delegate them based on "real world" measurements like the existence of a death certificate? Are "heartbeat" services like deathswitch.com really the best solution?

2. *Do the dead have a right to privacy?* It does not appear to be the case, but they may still have property rights; the CNET article "Taking Passwords to the Grave" [17] quotes Marc Rotenberg, executive director of the Electronic Privacy Information Center: "The so-called 'Tort of Privacy' expires upon death, but property interests don't," he said. "Private e-mails are a new category. It's not immediately clear how to treat them, but it's a form of digital property."

3. Given that the most likely legal framework to apply is that of property rights, *How does digital identity information compare with other physical "material" property belonging to the departed?*

4. *How large are current digital identity footprints?* A well-done user study exploring this data might shed light on the complexity of managing multiple identities.

5. *Do the dead have the right to specify the enforcement of compartmentalization of their digital footprint?* It seems clear that users engaging in any form of estate planning should have firm footing to specify how to dispose of their digital identity.

6. *Who "owns" a set of digital credentials: the user or the service they are meant to authenticate to? If a third party generated them (e.g., a browser plugin on behalf of a company or developer), does the third party have any rights?* We may be wading into legal murkey waters here (we just don't have the background to know) – but it seems like any comprehensive definition of "identity" (like the one we gave in Section 1.3) would likely include elements that service providers would think of as *their* property, setting up a conflict over control of these assets.

7. *What are the usability concerns of an identity protection system meant to ease transition of digital identity information upon the event of the owner's death?*

8. *Under what conditions should a provider of such an identity container storage solution be compelled to release this private data? What is the legal framework that should be applied?*

9. *How do survivors prove to the ID container provider their identity?* Some services offer to provide data to survivors or executors, but only after a significant amount of paperwork.

10. *What are the reasonable constraints on the cost of this service? Is an insurance model the most ethical?* A centralized identity management solution seems distasteful (witness the reaction to the US National Strategy for Trusted Identities in Cyberspace), but for a marketplace of such services, can they ethically make money when they might be seen to be gouging the bereaved? Does an insurance model for the deceased work?

11. *How liable should the identity container provider be for disclosure? Do special penalties apply?* If there is a viable business or public service in running such a provider, do they have a special responsibility to procure "above average" protection, auditing, and mitigation techniques against cyberattack?

12. *Is adding yet another layer of management to digital identity just compounding the problem?* People already struggle with identity overload (and compensate in ways like password reuse and weak passwords); although a cloud-based identity provider framework seeks to decrease this cognitive load, adding yet another layer of indirection to a fractured authentication landscape might be a cure worse than the disease.

Our identity is different than existing web services; we offer fine-grained control rather than an unlocked vault.

6. RELATED WORK

A significant amount of work exists on the topic of authorization and authentication; this subfield is a staple of the information security discipline. This paper deals with the usability of authentication schemes (more precisely, digital identity management schemes). Recently, the topic of usable security — particularly usable authentication schemes — has received a great deal of attention. Graphical password schemes were suggested as an easier-to-remember alternative to traditional weak passwords, but even these schemes have weaknesses suggest Biddle et al. [1]. The PassThoughts [22] paper from NSPW 2005 explored the feasibility of a mentally-driven approach to authentication.

6.1 Identity Management Failures

It seems that however much attention we pay to creating usable authentication mechanisms, *identity management* remains a challenging task. The recent Epsilon episode [21] shows us a failure mode of outsourcing user identity information to a third party. From Target and Best Buy to Citigroup and Marriott, valid user names and email addresses were disclosed by a single intrusion [4].

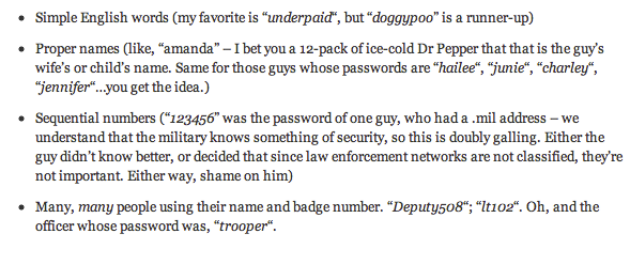
Recent headline-grabbing attacks by movements like Anonymous and LulzSec demonstrate the ease with which PII and account information can be obtained and released, along with reminders of how poor real-world password practices are (see, e.g., Figure 3; this screen capture was taken from the "Police-Led Intelligence" blog [19]). In other LulzSec-related news, Troy Hunt performed an analysis of Gawker and Sony passwords, finding, among other things, that 50% of passwords were less than 8 characters, only 4% of those passwords contained three or more types of characters (and only 1% included a non-alphanumeric type), and fully "two-thirds of people with accounts at both Sony and Gawker reused their passwords."[4]. An earlier companion article lists the 25 most popular passwords for Gawker and rootkit.com, and these two lists bear a great deal of similarity to the Sony set[5].

6.2 Death and Computing

In recent years, computer scientists and system designers have begun to understand the implications of death as it affects the social, technological, and personal dimensions of computing. Human-computer interaction (HCI) researchers have recently embarked on a series of studies seeking to unravel the complexities associated with death and computing. A CHI 2010 workshop ("HCI at the End of Life: Understanding Death, Dying, and the Digital")[6] explored this topic and was organized by one of the co-authors of this paper.

Massimi and Charise first drew attention to this area by envisioning a system design process called "thanatosensitive design" which

[4] http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html
[5] http://www.troyhunt.com/2011/03/only-secure-password-is-one-you-cant.html
[6] http://www.dgp.toronto.edu/~mikem/hcieol/



- Simple English words (my favorite is "*underpaid*", but "*doggypoo*" is a runner-up)
- Proper names (like, "amanda" – I bet you a 12-pack of ice-cold Dr Pepper that that is the guy's wife's or child's name. Same for those guys whose passwords are "*hailee*", "*junie*", "*charley*", "*jennifer*"...you get the idea.)
- Sequential numbers ("*123456*" was the password of one guy, who had a .mil address – we understand that the military knows something of security, so this is doubly galling. Either the guy didn't know better, or decided that since law enforcement networks are not classified, they're not important. Either way, shame on him)
- Many, *many* people using their name and badge number. "*Deputy508*"; "*lt102*". Oh, and the officer whose password was, "*trooper*".

Figure 3: ***An overview of some passwords used for the Missouri Online Training Academy.*** **This is just one instance in an overwhelming chain of evidence that people and passwords just don't mix – admirably demonstrated better than limited user studies.**

involves insights from the humanities and social sciences to actively engage with death as part of the design concept [15]. Indeed, death is an issue so immense that it often requires the expertise of multiple disciplines, including law, psychology, medicine, social work, and more. Researchers in human-computer interaction have suggested technology design at the end of life be framed in an approach borrowed from development psychology - that of looking at the human lifespan [16]. In so doing, stakeholder groups and important themes are highlighted. This framing also suggests that the individual's orientation towards death be considered throughout their own, and across multiple, lifespans. The application areas and needs throughout the lifespan shift; for example, writing a will is an activity often seen as impractical during youth, but immensely important as one grows older.

Beyond framing the space, HCI researchers have also sought to understand the social processes and tools that are involved during bereavement. One study investigated how personal technologies such as PCs and mobile phones are handled following a death in the family, and found that inheritance of such technologies is a complicated and difficult process, with passwords and biometrics commonly causing problems in accessing crucial data postmortem [13]. At the same time, these technologies symbolize a relationship which survivors continue to cherish, and they use technologies to continue the relationship in many ways. For example, Odom et al. describe a woman who buried her loved one with his cell phone so that she can continue to send him text messages [18]. The unique needs of the bereaved, and how technologies might be sensitively designed around these needs, has also been investigated through focus groups and interviews with bereaved parents and thanatology professionals [14]. One specific need from this study included the desire to be sheltered from others and the world immediately following a death, with the suggestion that we design technologies to shelter as much as they might connect.

Social networking websites such as MySpace and Facebook similarly permit relationships to endure past death. One study of MySapce found that the bereaved employ these websites to maintain rituals and write to the deceased, with predictable patterns of use during special occasions such as birthdays, death days, holidays, and so on [3]. Textual messages posted to profiles of the deceased comprise the majority of the interaction on such sites. In a recent linguistic analysis of messages posted to the walls of deceased Facebook users, Getty et al. found that several forms of grieving activities (e.g., sharing stories, expressing emotion) traditionally performed at memorial services are now taking place on these sites [8]. They place this finding in terms of Goffman's "dramaturgical" orientation towards social performance, which describes "front stage" and "back stage" activities that work together to create social situations [9]. In so doing, we see that many back stage activities (e.g., expressions of grief) are becoming visible to larger audiences on these social networking websites, alongside other more culturally acceptable forms of mourning. In the case of Canadian author and blogger Derek K. Miller [20], his friends and family used his pre-written last blog post as part of the grieving process.

Still other work has focused on what death means at a more cultural, widespread level. Technology plays a role in the recording, storage, curation, presentation, and stewardship of cultural histories. The Spomenik project - a form of "pervasive monument" - for example, allows mobile phone users to retrieve location-specific information about the mass grave sites from Stalinist purges of Slovenia and Yugoslavia in the 1940s [12]. Other researchers have used digital technologies to capture, organize, and disseminate testimonials from the Rwandan Genocide, remarking on the set of methods needed for designing multi-lifespan information systems [7].

Commercial products have also been designed to accomodate the unique needs that accompany death in the digital age. For example, companies such as Entrustet permit users to upload sensitive information with the assurance that the information will be delivered to designated people upon the user's death (`http://www.entrustet.com`). `Deathswitch.com` allows users to sign up for prompts to ensure that the user is still living; in the event that the user does not respond to the prompt in a timely fashion, the web service will automatically send out emails to designated parties. Other websites offer users the opportunity to plan out their own funerals (e.g., `http://www.memorialhelper.com`).

6.3 Advice

Recent articles consider best practices for keeping track of digital identity assets after death. Lifehacker [6] recommends making a list of your accounts, reviewing them to determine which you might want to survive or "go dark," and placing the authentication credentials on a USB token along with detailed instructions about actions to take with each account. A 2006 CNET article [17] describes advice from estate planners to put this information in an estate planning document (where it will have legal force). The recent Wall Street Journal article "PINs that Needle Families" [10] prescribes similar advice. We note that although this approach (writing authentication credentials down on paper) seems appealing and intuitive, it only provides a static snapshot of your digital identity.

7. WORKSHOP DISCUSSION

The lively workshop discussion explored different directions and attempted to understand how this topic might present new and unique security and usability challenges.

The discussion began with a brief, informal straw poll of workshop participants as to how large they thought their digital footprint was in terms of number of accounts; answers seemed to fall into two clusters: 19 responses in the 100 to 750 range and 7 responses in the 50 to 80 range, with one guess at around 1000 and one person declining to answer.

Our moderator, Richard Ford, asked what our definition of digital footprint was, and we moved to our slide with the definition from Section 1.3.

The question arose as to how much control you actually have over your digital assests after your death; we highlighted the advice from the CNET [17] suggesting the theory that property rights may persist, but Steve Greenwald asserted that all rights cease when you die, whether property or privacy.

During the ensuing discussion, we highlighted the point that people will have to deal with this issue more and more in the future;

Angelos Keromytis suggested that perhaps we were really advocating a form of "family-based key escrow", to which we concurred.

One participant asked whether there were similarities to the garbage collection process; we felt this might be a bit of a stretch of the analogy.

Lizzie Coles-Kemp suggested that this paper was closely related to the activity of the digital curation community (in both traditional and "active" forms), but they were not looking directly at authentication techniques. We certainly agreed. She also made the point that some social institutions are set up to deal with power of attorney while others were not. We feel this reinforces one of our key points: that no uniform, cohesive approach exists to this problem.

MEZ pointed out that companies often have explicit rules and business processes to deal with such events and eventualities; we concurred, but suggest that they are out of scope: money is at stake and they have evolved and implemented the necessary structures to take care of their slice of someone's authentication footprint. The issue in this paper is that families and friends seldom have a workflow process for dealing with someone's death.

One participant asked about what happens when a company holding some of your digital footprint itself ceases to exist; we admitted that the ownership rules here are murky (this is one of the potential issues we list in Section 5).

Someone made the point that personal security figures into most security scenarios: now, by offloading crendential management, the risk to life and limb might decrease in favor of a break-in at the remote storage facility.

Jeremy Epstein suggested that one way to influence the NIST NSTIC was to select providers that had a specific policy for this issue.

As the discussion came to a close, there was some agreement that there might be some very interesting usable security issues lurking here, especially with the proposal to create an identity mediator and make delegation natural. We also received links to some interesting projects, including an EU project (www.primelife.eu) and (digitaldeathday.com).

8. CONCLUSION

Many information security paradigms seem to ignore the human element in security problems and scenarios. Even disciplines that take human interaction into account (e.g., HCISec or usable security) seldom examine long-term phenomena.

A good expression of this paradigm is in the eventual shift of large parts of our society and economy into the online realm (e.g., banks that are completely online): it is likely that we will have to deal with organizations electronically.

The accrual of a heterogeneous, distributed digital identity footprint presents unique and interesting authentication, authorization, and privacy issues — particularly related to how such an identity collection should be retired after a person dies.

Acknowledgments

We appreciate the reviewers' comments and the guidance of our shepherd, Michael Franz. We also appreciate the responses and feedback we received during the workshop: we apologize in advance if we mis-remembered or misrepresented anyone's comments or point of view. Thanks also to the scribes for our session, Matt Bishop and Cormac Herley.

Locasto acknowledges the support of Canada's NSERC (Natural Sciences and Engineering Research Council) through a Discovery Grant. Massimi acknowledges support from the GRAND NCE (a Canada Network Centre of Excellence).

9. REFERENCES

[1] BIDDLE, R., CHIASSON, S., AND VAN OORSCHOT, P. Graphical Passwords: Learning from the First Twelve Years. *ACM Computing Surveys 44*, 4 (2012).

[2] BRIGHT, P. Anonymous Speaks: the Inside Story of the HBGary Hack, February 2011. http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars.

[3] BRUBAKER, J. R., AND HAYES, G. R. "we will never forget you [online]": an empirical investigation of post-mortem myspace comments. In *Proceedings of the ACM 2011 conference on Computer supported cooperative work* (New York, NY, USA, 2011), CSCW '11, ACM, pp. 123–132.

[4] CBCNEWS. Air Miles Among Firms Hit By Huge Data Breach, April 2011. http://www.cbc.ca/news/business/story/2011/04/05/business-data-breach.html.

[5] CENTER, T. H. How to Contact Twitter About a Deceased User. http://support.twitter.com/groups/33-report-a-violation/topics/122-reporting-violations/articles/87894-how-to-contact-twitter-about-a-deceased-user.

[6] FITZPATRICK, J. What Should I Do About My Virtual Life After Death?, August 2010. http://lifehacker.com/5617683/what-should-i-do-about-my-virtual-life-after-death.

[7] FRIEDMAN, B., NATHAN, L. P., LAKE, M., GREY, N. C., NILSEN, T. T., UTTER, R. F., UTTER, E. J., RING, M., AND KAHN, Z. Multi-lifespan information system design in post-conflict societies: an evolving project in rwanda. In *Proceedings of the 28th of the international conference extended abstracts on Human factors in computing systems* (New York, NY, USA, 2010), CHI EA '10, ACM, pp. 2833–2842.

[8] GETTY, E., COBB, J., GABELER, M., NELSON, C., WENG, E., AND HANCOCK, J. I said your name in an empty room: grieving and continuing bonds on facebook. In *Proceedings of the 2011 annual conference on Human factors in computing systems* (New York, NY, USA, 2011), CHI '11, ACM, pp. 997–1000.

[9] GOFFMAN, E. *The presentation of self in everyday life*. Penguin psychology. Penguin, 1990.

[10] GREENE, K. PINs That Needle Families, July 2011. http://online.wsj.com/article/SB10001424052702304567604576456182693233372.html.

[11] IOANNIDIS, J. Fighting Spam by Encapsulating Policy in Email Addresses. In *Proceedings of the ISOC Symposium on Network and Distributed Systems Security* (2003).

[12] KOSEM, J., AND KIRK, D. Spomenik: Monument. In *CHI 2010 Workshop on HCI at the End of Life* (New York, NY, USA).

[13] MASSIMI, M., AND BAECKER, R. M. A Death in the Family: Opportunities for Designing Technologies for the Bereaved. In *Proceedings of the 28th International Conference on Human Factors in Computing Systems* (New York, NY, USA, 2010), CHI '10, ACM, pp. 1821–1830.

[14] MASSIMI, M., AND BAECKER, R. M. Dealing with Death in Design: Developing Systems for the Bereaved. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems* (New York, NY, USA, 2011), CHI '11, ACM, pp. 1001–1010.

[15] MASSIMI, M., AND CHARISE, A. Dying, Death, and Mortality: Towards Thanatosensitivity in HCI. In

Proceedings of the 27th international conference extended abstracts on Human factors in computing systems (New York, NY, USA, 2009), CHI EA '09, ACM, pp. 2459–2468.

[16] MASSIMI, M., ODOM, W., BANKS, R., AND KIRK, D. Matters of life and death: locating the end of life in lifespan-oriented hci research. In *Proceedings of the 2011 annual conference on Human factors in computing systems* (New York, NY, USA, 2011), CHI '11, ACM, pp. 987–996.

[17] MILLS, E. Taking Passwords to the Grave, September 2006. http://news.cnet.com/Taking-passwords-to-the-grave/2100-1025_3-6118314.html.

[18] ODOM, W., HARPER, R., SELLEN, A., KIRK, D., AND BANKS, R. Passing on & putting to rest: understanding bereavement in the context of interactive technologies. In *Proceedings of the 28th international conference on Human factors in computing systems* (New York, NY, USA, 2010), CHI '10, ACM, pp. 1831–1840.

[19] SELBY, N. Analysis: 70 Law Enforcement Sites Attacked, July 2011. http://policeledintelligence.com/2011/08/01/analysis-70-law-enforcement-sites-attacked/.

[20] SILVER, K. Blogger Announces Own Death After Battle With Cancer, May 2011. http://www.cnn.com/2011/WORLD/americas/05/08/-canada.blogger.death/index.html?hpt=T2.

[21] SNYDER, B. Epsilon E-Mail Hack: How You Can Protect Yourself, April 2011. http://www.networkworld.com/news/2011/041111-epsilon-e-mail-hack-how-you.html.

[22] THORPE, J., VAN OORSCHOT, P., AND SOMAYAJI, A. Pass-thoughts: Authenticating With Our Minds. In *Proceedings of the New Security Paradigms Workshop* (2005).