The Shoebox and the Safe: When Once-Personal Information Changes Hands

Manas Tungare
Google, Inc.
manas@tungare.name

ABSTRACT

This paper presents several examples where one user's personal information is accessed by another, without the consent of the owner, or without the capability of the owner to consent to such sharing. While intentional sharing of information at home as well as at work has been studied in detail, there is extremely limited understanding about the practices, dimensions and models of unintentional sharing. Laws and policies that were developed with paper and other non-digital archives in mind are being found to be inadequate for addressing the challenges that digital personal information brings. Worse, those laws are being enforced in inconsistent ways, prompting lawsuits. Posthumously shared information brings up questions that have not been addressed before. This paper starts by noting examples of posthumous sharing and sharing without consent, proposes models and dimensions for understanding it, and concludes by proposing research questions that need to be addressed by the wider PIM community.

INTRODUCTION

Personal information, by its very definition, is information that belongs to a single user. But this boundary has been pushed more and more, as social sharing of information gains traction. What used to be stacks of papers and files under a user's desk or in her office are now all stored digitally. Digital artifacts, by their very nature, are much more amenable to sharing and movement among people than their analog predecessors. Just as the presence of digital tools brought along new problems in Personal Information Management, so does the introduction of social channels.

What happens when personal information changes hands unintentionally? What happens when knowledge that was meant for the consumption of a single individual is now available to a wider audience? Knowledge about other people's personal information is powerful. The destinies of wars and empires have changed drastically when private information changed hands, as politicians and historians are well-aware. Even in the modern day, political ambitions are shattered when intimate personal details of candidates seeking office are made known publicly.

This paper seeks to examine the questions that arise when personal information changes hands. In this paper, I focus on posthumous sharing and unintended sharing, two models of sharing that have not yet been adequately studied, and propose several dimensions for understanding this sharing.

POSTHUMOUS SHARING OF PERSONAL INFORMATION

It is not uncommon for a deceased person's worldly belongings to be passed on to their next of kin. Photographs, video tapes, paintings, and other tangible memories have had a tradition of being passed on. For those that we revere, such artifacts are preserved as a monument to the eternity of the ideals they lived for. Sometimes, these artifacts are curated by the now-deceased or by their confidantes, so as not to cause embarrassment or concern when they are made widely available. Also, these have been filtered to remove the trivialities of daily life, while leaving the truly memorable moments intact.

With perpetually-archived digital information, however, all of this changes significantly. In cases of sudden or accidental death, the next of kin might have no access to this private information if all of it was locked behind a password known only to the deceased. At the other extreme, it is possible for deeply intimate daily conversations of a recently-deceased person to be made known widely. Society is not used to either of these two extremes, and thus does not have the tools and/or vocabulary to address them. The emotional sensitivity and unpredictability of the death of a near one makes it difficult for researchers to recruit and study subjects who might be able to provide some insight into this problem [5].

Lack of Uniform Policies, Protocols, and Laws

In 2007, Virginia Tech witnessed a disastrous massacre on campus when an armed gunman shot 32 victims at point-blank range[1]. While the entire community was coming to grips with a deeply personal tragedy so close to home, I received a call from the brother of one of the victims. The victim had an active profile on a social networking site, and upon hearing about the shooting, the publicly-visible page was being inundated by messages of condolence from shocked friends and family. While this was well-intentioned, this issue was understandably a further cause of grief for the family. The brother wanted to get this profile deleted.

[1] http://www.nytimes.com/2007/04/16/us/16cnd-shooting.html

Submitted for review to the Fifth International Workshop on Personal Information Management (PIM 2012), Seattle, WA, USA.

Eventually, as I communicated with those in my professional network who had the power and ability to address this request, I realized that there were no set protocols, uniformed industry policies, or laws to address how personal information should be handled when its primary user ceases to be: Yahoo! requires users to obtain a court order to release private information of deceased users [3], while AOL does not.

Controlled Posthumous Sharing

A diary is perhaps the most personal corpus of information one could create. However, the posthumous release of a Jewish girl's personal diary chronicling the Nazi occupation is now known as one of the greatest literary works of the last century: The Diary of Anne Frank. We will never know if Anne would have agreed with her father's decision to release her personal diary for wide public consumption.

Mark Twain, the 19th century humorist, intended his biography to be kept from public view for 100 years after his death. In 2010, a century after his death, parts of his biography have been released to huge audience interest.

There are several other examples of great artistic works published posthumously (including Franz Kafka, J. R. R. Tolkien, Vincent van Gogh—all the way back to Niccolò Machiavelli in the 16^{th} century) but these would not be considered personal information, and hence not under the purview of this discussion.

Biometric Authentication

Biometric authentication refers to the use of biological and physical characteristics of a user as the means for authentication. Techniques such as finger prints, retinal eye scans, and others are commonly used at an institutional level where a high level of physical security is required. While this is not yet widely used to secure personal information, it is likely that such information will be permanently lost when the owner is no more to decrypt it.

Research Questions

How does posthumous sharing of personal information compare to age-old practices around the same practice? How does the availability of huge archives, including trivialities and special moments, affect user's choice of whether or not to share their worldly belongings, and how much of it? What part, if any, can be legislated to cover situations where the deceased person's intentions are not explicitly known after death?

SHARING WITHOUT CONSENT

Personal information shared without consent is essentially unauthorized access. It may be among families, friends, colleagues, or with unknown entities such as thieves and law enforcement.

Sharing Among Relatives and Friends

Information sharing among close family, friends, and coworkers is well-understood and expected. Some spouses share computers and passwords, giving each other unfettered access to their information, while others choose to maintain two individual spaces plus one shared space for their mutual information. But not all such domestic sharing is with mutual consent. Below are several examples of information being shared against the will of the person who owns it.

Between Minors and Parents

Parents sometimes require that their young children share their passwords, emails, social networking profiles, and other personal information with them as a precondition to being allowed to use the home computer. While children are in the process of navigating their way through technology and information and the social issues related to them, this is a legitimate way to introduce them to these issues with parental consent and a guiding hand.

Between Spouses and Domestic Partners

Smart-phones include features such as Google Latitude and Apple's 'Find My iPhone' which let users locate their cell phones from a remote location using GPS technology. Although the stated use of this feature is to locate the phone in case it is stolen, there is nothing preventing this information to be used in other ways, as a New York City couple recently found out[2]. The husband installed this app on a phone that he had recently purchased for his wife. He soon realized that the location sent by the phone did not match where she said she was at that time, which confirmed his suspicions that she had been less than faithful to him.

During Illness or While Incapacitated

During illness or when one is otherwise incapacitated, it may be necessary for others to gain access to one's personal information for any of several purposes: to address financial commitments such as pending bills, to inform concerned third-parties (e.g. their employer) about the sick person's status, or simply acting as that person's assistant for the temporary period of illness.

Sharing at Work or School

The practices around sharing corporate information in work and school environments have been studied quite deeply in the field of CSCW (Computer-Supported Collaborative Work). In addition to corporate information, some employers and schools demand access to personal information as a precondition for continued employment, despite the fact that such a practice exhibits a lack of respect for basic rights of the employee or student.

In early 2011, the Maryland Division of Corrections had a policy that required everyone seeking employment to submit to a background check that included sharing their social networking site passwords, clearly a privacy violation. The American Civil Liberties Union sued the Division on behalf of a job applicant [1], which led to this practice being discontinued [4]. Mississippi's Pearl High School found itself the target of a lawsuit when teachers sought access to a minor student's Facebook account [6].

[2]http://forums.macrumors.com/showthread.php?t=1254206

These cases illustrate that even state departments and government institutions are struggling to understand and respect a person's rights to privacy of their own personal information. This would not have been the case if this personal information resided on a user's home computer. But the fact that it is on the Web leads them to believe that it is somehow less personal and more accessible to prying eyes.

Scams, Phishing, Data Theft, and Other Crimes

As more and more personal information moves online, it presents an easier target for criminals. Simply knowing someone's online banking password is enough to let a skilled criminal siphon off their funds. Nearly every month, there is a news story about credit card information stolen from an institution that was lax in safeguards against data theft. Identity theft, where secret personal identifying information is used to commit financial fraud under the name of the original person is an increasing concern.

Billions of emails are sent each day to users' mailboxes that are crafted to look like they came from a bank or other financial institution which try to lure users to enter their real passwords on a fake site, in a technique known as Phishing. The reason these scams exist is because they work. Computer viruses are no longer written simply for fun: they are the latest technique in capturing users' passwords, which are then sent back to whoever wrote the virus. The authors are no longer bored computer programmers, but well-organized crime rings.

Having access to another person's email password is the doorway to all sorts of financial scams. Passwords to third-party sites are often configured to be reset by sending a verification email to the user's email account. More complex scams involve sending emails to the victims' contacts, saying that the victim is currently in a foreign country, unable to communicate further, and asks for money to be sent to them urgently via non-trackable means. Many savvy users fall prey to this tactic, because email (and typed text in general) is an easy way to hide the identity of the sender.

Nation-states have been known to gain illegitimate access and to snoop on the email communications of those that are deemed to be a threat to the controlling authority of the ruling party.

Law Enforcement

The Fourth Amendment[3] to the Constitution of the United States grants citizens the right to be secure against unlawful searches, but recent judiciary precedent is seen to be leaning towards a lower burden-of-proof requirement to gain access to users' personal information. During crime scene investigations, forensic experts often tend to seize personal files and documents, including those stored locally or in the cloud.

[3]"*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"

In recent court proceedings, a divorcing couple was instructed by the judge to trade their Facebook passwords after the husband suspected that more evidence would be available in the wife's online activity trail to support his claim to custody of the children [2].

Various data retention laws require corporations to retain logs of information such as individual employees' email and calendar data, which tread the border between personal and corporate information. Litigation holds placed on certain employees require them to keep an archive of personal information until such a hold is lifted.

Thus, law enforcement can force otherwise private information to be released to the public domain, despite all measures of secrecy that might have been taken by the user. This did not used to be the case when most communication was over ephemeral channels such as face-to-face and over the telephone. This is a problem that has clearly been exacerbated by the digitization of information.

MODELING UNINTENDED SHARING

Below is a first attempt at characterizing these modes of unintended sharing: these are only preliminary models that suit the exploratory nature of a position paper.

The Shoebox and the Safe

I use the term "shoebox" (referring not necessarily to an actual shoebox, but to a traditional container of old photographs, souvenirs, and other knick-knacks of sentimental value) to refer to a corpus of information that is intended for wider sharing by an individual under certain clearly-defined circumstances.

In contrast, I use the term "safe" (the noun form; a locked metal box commonly used to store jewelry, valuables, and important possessions) to refer to information that is sometimes shared with others against the will of the user.

When personal information is created, users tend to place it into one of these bins when they have a specific intention about how it should be shared. A third bin can be labelled as the 'Everything Else' bin, when no specific mode of sharing is intended. Information in the shoebox automatically passes along to others; information in the safe should ideally not. This model is also indicative of others' interest in one's personal information: a thief or law enforcement official is much more likely to be interested in the contents of a safe than in the contents of a shoebox. A family member or close friend is much more likely to want to peruse the contents of the shoebox.

In addition to this simplistic model, there are several other dimensions along which such sharing can be studied.

Voluntary versus Involuntary

While this paper focuses on involuntary sharing of personal information, some cases are borderline: who is to decide whether the case of the college principal requiring his students to submit their Facebook passwords constitutes a case

of voluntary disclosure or involuntary search and seizure? Burglaries and law enforcement-related information searches are clearly involuntary, while sharing within families is likely to be voluntary. Posthumous sharing may be either.

Copy versus Move

This refers to whether the original user continues to have access to his/her information after it has been made available to another. Digitized information makes it easier for the same piece of information to exist in multiple places, which makes it possible for the original user to be left completely unaware that any unauthorized access has occurred. This can be more dangerous than losing the information in the first place, especially in situations involving espionage where the primary actor may not realize that her communication is being eavesdropped on.

Limited Scope versus Everything

There is great value in exposing limited facets of one's personal information with selected circles. E.g. employees can often see each other's calendars as a routine manner of scheduling meetings, and spouses often share some limited information by default. Problems occur when the scope of sharing is violated. Newer authorization protocols such as OAuth support limited revocable sharing as an explicit design goal.

Limited Time versus Perpetual

When traveling, it is acceptable for neighbors to receive mail on behalf of the travelers, and perhaps even act on time-sensitive material. However, the social contract mandates that such sharing would be for a limited time only, and must be discontinued when the travelers return home.

Limited Audience versus Public

Digitized information has made it easier for one's personal information being made available to a vast public audience intentionally or unintentionally. Politicians with lascivious tendencies, starlets indulging in promiscuous behavior behind closed doors, and many teenagers with camera-equipped smart-phones have found this out the hard way when private photos that were intended for a much closer audience—which would have been perfectly legitimate if they had remained that way—leaked onto the public Internet. Public-by-default settings on social networks such as Facebook and the ubiquity of digital cameras have made this genre of cases much more likely to happen through only a minor mistake on part of the user or sharer. This is one area where the shoebox/safe classification fails to be granular enough to capture the nuances of the sharing.

Intent: Malicious, Helpful, Curiosity, or Other

Family members usually access one's digital remains out of curiosity, respect, and remembrance. Criminals have active malicious intent in obtaining access to private information. Some, like WikiLeaks, have a broader agenda in disseminating private information. Others such as the hacker group Anonymous publish private information to humiliate entities whose policies they disagree with.

RESEARCH QUESTIONS

What are the dimensions against which such sharing may be understood and studied? How can it be prevented?—if at all. Until the dawn of the information age, most information was ephemeral, and/or did not have a global reach. How does the current practice of archiving everything till the end of time on devices with increasing storage capacities affect such sharing? How does the availability of a global Internet that allows anonymous sharing sans liabilities affect this sharing? What may be done to inform the legal landscape around unauthorized sharing and sharing without consent? What are the broader societal implications of publicly sharing once-personal information? Are the private lives of politicians their own business, or do voters have a right to know certain aspects of their private lives? At a time when individuals are encouraged to store and access their information from the cloud, how does this affect the privacy of their information when law enforcement officials come knocking? The point of raising these questions in this paper is not to answer them, but to provoke discussion about them.

REFERENCES

1. ACLU of Maryland. ACLU says division of corrections' revised social media policy remains coercive and violates "friends" privacy rights. http://www.aclu-md.org/aPress/Press2011/041811_Facebook.html, April 2011.

2. K. Hill. Judge orders divorcing couple to swap facebook and dating site passwords. http://www.forbes.com/sites/kashmirhill/2011/11/07/judge-orders-divorcing-couple-to-swap-facebook-and-dating-site-passwords/, November 2011.

3. J. Hu. Yahoo denies family access to dead marine's e-mail. http://news.cnet.com/Yahoo-denies-family-accessto-dead-marines-e-mail/2100-1038_3-5500057.html, December 2004.

4. A. Madrigal. Maryland agency stops asking interviewees for Facebook login. http://www.theatlantic.com/technology/archive/2011/02/maryland-agency-stops-asking-interviewees-for-facebook-login/71582/, February 2011.

5. M. Massimi and A. Charise. Dying, death, and mortality: towards Thanatosensitivity in HCI. In *Proceedings of the 27th international conference extended abstracts on Human factors in computing systems*, CHI EA '09, pages 2459–2468, New York, NY, USA, 2009. ACM.

6. J. van Grove. Abuse of power: High school admins coerce cheerleader for Facebook password. http://mashable.com/2009/07/29/cheerleader-lawsuit/, July 2009.