Sensible Privacy: How We Can Protect Domestic Violence Survivors Without Facilitating Misuse

Budi Arief, Kovila P. L. Coopamootoo, Martin Emms, Aad van Moorsel
School of Computing Science, Newcastle University
Newcastle upon Tyne NE1 7RU, United Kingdom
{budi.arief, kovila.coopamootoo, martin.emms, aad.vanmoorsel}@ncl.ac.uk

ABSTRACT
Privacy is a concept with real life ties and implications. Privacy infringement has the potential to lead to serious consequences for the stakeholders involved, hence researchers and organisations have developed various privacy enhancing techniques and tools. However, there is no solution that fits all, and there are instances where privacy solutions could be misused, for example to hide nefarious activities. Therefore, it is important to provide suitable measures and to make necessary design tradeoffs in order to avoid such misuse. This short paper aims to make a case for the need of careful consideration when designing a privacy solution, such that the design effectively addresses the user requirements while at the same time minimises the risk of inadvertently assisting potential offenders. In other words, this paper strives to promote "sensible privacy" design, which deals with the complex challenges in balancing privacy, usability and accountability. We illustrate this idea through a case study involving the design of privacy solutions for domestic violence survivors. This is the main contribution of the paper. The case study presents specific user requirements and operating conditions, which coupled with the attacker model, provide a complex yet interesting scenario to explore. One example of our solutions is described in detail to demonstrate the feasibility of our approach.

Categories and Subject Descriptors
K.4.1 [**Computers and Society**]: Public Policy Issues – *Abuse and crime involving computers, Privacy.*

General Terms
Security, Human Factors.

Keywords
Privacy; anonymity; tradeoffs; privacy enhancing technologies; privacy in mobile systems; privacy threats; personal privacy; domestic violence; survivors.

1. INTRODUCTION
The pervasiveness of digital technology makes our lives easier by enabling access to information and services whenever and wherever it is required. However, technologies used to access services leave a trail of "electronic footprints" that can be followed by users to keep track of their activities, by service providers to provide personalised services to their customers, and by authorities to identify and track down perpetrators in case of misuse of technology. This leads to issues related to privacy, which has become more prominent lately, especially as a result of the Snowden revelation [1].

Consequently people are growing more aware about the need to protect the privacy of their data. Furthermore, there are cases where privacy infringement could lead to serious consequences such as loss of jobs or life [2]. As such, many researchers have spent efforts into creating various techniques and tools to enhance the privacy of stakeholders concerned.

One poignant scenario is the case of domestic violence, in which survivor's electronic footprints might be tracked by their abuser as part of the abuser's attempt to monitor and exert control over the survivor, strengthening the cycle of harm to the survivor. In this scenario, survivors might not have the technical ability to cover their tracks and indeed, they often have less confidence in using technology compared to their abusive partners [3]. The fear of being discovered and of suffering more abuse contributes to preventing survivors' access to support services and maintain the abusers' physical and psychological control over them [4]. Therefore, as suggested by the requirements compiled by van Moorsel et al. [5], a privacy approach must be accessible, usable and useful for survivors and provide the confidence and assurance that seeking help is at a lower risk than enduring abusive relationships.

On the other hand, it is sometimes necessary for privacy to be *breach-able*. As with any technological solution, there is a risk that some individuals might circumvent the original purpose to misuse the solution in nefarious activities. Sharing sexual abuse images of children using the "Darknets" [6] is one notorious example of such misuse. By hiding behind this anonymisation service, perpetrators might feel more confident that their activities are not detectable by law enforcement agencies, or at least it becomes a very tough challenge for child protection officers to identify and arrest the perpetrators.

With this context in mind, we would like to propose a concept of *sensible privacy* with tradeoffs that strive to get a balance between privacy, usability, and accountability. This is not to the level of implementing backdoors for government or law enforcement agencies to snoop in, but instead, a suitable attacker model needs to be developed so that a solution can be devised in a way that raises the barrier for the attackers, but not prohibiting law enforcement officers to carry out their investigative duty.

> DEFINITION 1 (SENSIBLE PRIVACY) *In the context of this paper, sensible privacy refers to the combination of privacy tradeoffs between privacy and usability and privacy and accountability.*

Privacy literature covers a series of tradeoffs including those made by the user or as design decisions. User tradeoffs include cost in exercising privacy versus benefits [7], but could also include cost in terms of cognitive effort spent or trust-privacy tradeoffs relating to incentives [8]. Design decisions tradeoffs include privacy versus utility of data tradeoffs [9] or privacy versus accountability tradeoffs [10] also linked with privacy versus security [11]. Our definition of sensible privacy combines two of the design tradeoffs and is both sensitive to user requirements and caters for the potential of misuse. This approach does not limit the design to the requirements of only one group of stakeholders.

The rest of the paper is organised as follows: Section 2 looks back at the basic concept of privacy and presents related work, including a selection of popular existing privacy solutions. Section 3 serves as the core of the paper, describing a case study of designing solutions for domestic violence survivors with sensible privacy in mind. This section also presents the key challenges faced, the attacker model envisaged, a sample solution that addresses the tradeoff needs, and the lessons learned from this case study. Section 4 concludes the paper and outlines ideas for future work.

2. PRIVACY AND PRIVACY ENHANCING TECHNOLOGIES

Privacy is a behavioral and multi-dimensional concept: individuals dynamically manage their privacy according to different situations in social life. Privacy enables a dialectical state [12] that allows individuals to be both connected and autonomous. The interplay of needing both privacy and openness influences the decisions individuals make about the way they manage their information. As a consequence, they do not usually require complete privacy. Rather, they are happy to share information with others as long as certain social norms are met, that is contextual integrity of the shared information is maintained [13].

However the concept of "privacy" – especially in relation to the definitions proposed by previous research to explain it in terms of data minimisation, e.g. [14] – has a strong influence on the work presented in this paper. A terminology has been proposed to describe privacy in terms of data minimisation [14] in the systems domain; that is minimising the collection and processing of identifying information when using online services. Using this terminology, privacy is defined in terms of anonymity, unlinkability, unobservability, and undetectability. Anonymity supports the dialectical nature of privacy since it is the state in which an agent is able to engage in a transaction with another party while not being identifiable within an anonymity set consisting of senders, receivers and servers within a communication network. It also includes unidentifiability (that is observers cannot identify the agent), unlinkability (that is observers cannot link the agent to a specific message or action) and undetectability (that is observers cannot determine whether the message exists or not).

Many currently available privacy enhancing technologies and tools are examples of privacy-by-architecture designs [15]. Many serve the purpose of anonymising communication such as Onion Routing [16], Hordes [17], Crowds [18], Anonymiser [19], Tor [20] and authentication protocols for mobile scenarios [21]. Other anonymising techniques include anonymisation of records and logs [22] and cookie removal software [23]. As countermeasures against surveillance, Free Haven [24], remailers (such as mixmaster [25]) and Pretty Good Privacy [26] can be used, while live USB/DVD tools such as Tails [27] provide protection against the potential threat of keyloggers being present on the user's home computer. As mentioned before, Darknets [6] is a kind of privacy preserving service that is often tarred with the bad name associated with illegal activities such as sharing copyrighted materials or indecent images of children. This anonymous distributed peer-to-peer service is one example of how a good privacy solution could be misused to facilitate illegal activities.

To summarise, given the functional requirements of privacy, maximal anonymity might not be practically useful for individuals and could circumvent accountability. Also, although privacy is a universal requirement that enables individuals to maintain different types of interactions, for some individuals the consequence of a breach of privacy protection could be psychological or physical harm including death, as described in more detail in the next section with the case of survivors of domestic violence.

3. CASE STUDY: DESIGNING PRIVACY SOLUTIONS FOR DOMESTIC VIOLENCE SURVIVORS

A clear link has been established between issues of domestic violence and intimate partner cyber stalking [28][29]. Intimate partner cyber stalking refers to stalking conducted by current or ex-partner using a wide variety of information-based technology. The stalker or abuser has a high level of access to and knowledge about the habits of the survivor. As a result, intimate partner cyber stalking is a new and powerful weapon which adds to the ways in which the survivor can be controlled and/or coerced.

Through a collaboration with an independent charity dealing with domestic and sexual violence in the north east of England, we have been in contact with survivors of domestic violence. This collaboration highlighted the barriers faced by domestic violence survivors in trying to use technology to find support and help. The major concern is that survivors are often reluctant to seek help – either from friends and family or from support organisations – because they are afraid that such actions will attract attention and that they may risk further abuse if discovered. There is also a concern that survivors often do not know where to get help from or they are not aware about services that are available. These concerns motivate us to investigate and explore the needs and challenges faced by survivors in accessing support services, which among others boil down to the need to protect survivors' privacy while accessing online support services.

3.1 Challenges

Providing privacy solutions that are useful for and usable by everyone is practically an impossible task. We decide to focus on a group of users (domestic violence survivors), while keeping open the possibility of expanding the approach to other groups in society in general, and minimising the risks of our solutions being used for nefarious activities. Several key challenges have been identified below.

3.1.1 User considerations

- *Catering for non tech-savvy users*: users might lack the skills, awareness, or confidence in using technology in general, and privacy technology in particular.
- *Dealing with multiple devices*: there is a real challenge to keep the consistency of private information and privacy settings on different devices. These tend to have a non-uniform way to manage their privacy settings, therefore exacerbating the first key challenge above.
- *Considering user's psychological profile*: user's mental state could affect the effectiveness of the solution. While under duress and constant fear, it is inevitable that survivors might panic and struggle to use features that would normally be straightforward to use, or to miss certain precautionary routines.

3.1.2 Mitigating misuse

- *Minimising potential misuse of the solution*: users might twist the good features provided by the solution into something negative or even illegal. Privacy enhancing technologies are

not immune from this challenge, as demonstrated by the use of Darknets by paedophiles for sharing images of sexual abuse of children, as well as the relatively recent seizure of Bitcoins digital currency due to an alleged drug law violation [30].

3.2 Attacker Model

The main potential attackers are the survivors' partner (and abuser). Some key assumptions of these abusers are given below:

- They have access to or control of the (shared) computer at home and/or even the survivors' smartphones.
- They have sufficient computer knowledge (for example, they know how to check web browser history), but they are not a hacker or an expert in computer security or forensic.
- They may monitor the survivors' computer usage all the time, but they do not use a key logger or network sniffer. Nonetheless, it is expected that the attacker will be able to take control of the survivor's computer and/or smartphone after the survivor finishes using it to access domestic violence support websites, either blatantly (even by force) or discreetly.

Therefore one of the main aims of our proposed solutions is to remove traces of digital footprints associated with domestic violence support websites from any devices used by the survivors.

3.3 Sample Solution: Selective Sanitation of Smartphone History

The Selective Sanitation of Smartphone History app aims to allow survivors to freely access online resources whilst hiding their activities from their abusers. The objective of this solution is to automatically erase the digital footprints left behind when a survivor accesses specific domestic violence support websites, or when they make/receive a call (or send/receive a text message) to/from phone numbers associated to domestic violence support services. The app leaves intact all other history entries, thereby avoiding making it look like the phone has been cleaned. The way the app is designed reflects the key challenges outlined in Section 3.1, as well as the attacker model described in Section 3.2:

- The app is very easy to use; in fact it does not require user interaction at all once it has been installed on the smartphone. In order not to draw attention to itself (due to the very high likelihood that the abuser might demand the survivor to hand over their smartphone), the app is hidden behind an innocent front end, such as a game app or an image gallery app, so that it is not obvious for the abuser that the survivor has this app running on their smartphone.
- The app is designed to run on multiple Android platforms, and it has no adjustments/settings to worry about. The list of which websites or phone numbers to sanitise is currently embedded in the app, with future version envisaged to have this list hosted online with a feature to download the updated list discreetly when a new list becomes available.
- The effectiveness of the solution does not depend on the user's mental state. The app runs as a background service that is automatically turned on when the smartphone is started. It routinely carries out the sanitation actions every few minutes, so that the survivor is not required to remember about executing the sanitation actions.
- To minimise the potential risk of the app being misused to erase access history to illegal websites, the app does not go as deep as cleaning the SQLite database used for storing these history entries. In other words, forensics experts should still be able to piece back information from the SQLite database (a recent report [31] indicates that it is possible to recover data from Android devices even after a factory reset); however this should be enough to raise the barrier to prevent the expected attacker (the survivor's abusive partner) to find out about an attempt by the survivor to find help.

3.3.1 Other bite-size solutions

In addition to the solution described above, our approach consists of a number of complementary technologies that provide bite-size protection [4]:

- To distribute information to survivors, QR codes (that can be embedded on everyday things such as mugs and postcards) and NFC tags built in location-based service advertising in public places have been implemented.
- The QR codes are implemented as single-shot URL, which means that the first time the link is used, it will direct survivor to the domestic violence support website, but any subsequent access will be directed to an innocuous or safe page, such as the postcard maker's website.
- A secret graphical gateway has also been implemented to allow survivors to "remember" a support website without adding the link as a bookmark. This gateway avoids the obvious interactive feature of login-password: the application is disguised as an image gallery that displays a set of pictures, one of which authenticates the user when clicked in the right sequence at the right coordinates.

3.4 Sensible Privacy Recommendations

Taking into account the challenges and attacker model outlined in Sections 3.1 and 3.2, we propose *sensible privacy* as a design that would allow the solution to address the intended users' needs, while at the same time minimising the risks of the solution being misused for illegal or other harmful activities. We formulate the lessons learned for implementing sensible privacy as follows:

1. Account for the varying technical ability and psychological state of users.
2. Design privacy solutions that work straight out of the box, i.e. they do not need special knowledge or complicated set-up procedure.
3. Make sure the proposed solution is not self-defeating, i.e. the solution should not inadvertently cause more harm to its users.
4. Account for human nature and weaknesses, such as sharing information with family and friends, which might lead to a life-threatening situation.
5. Include not only one privacy mechanism, but rather a set of mechanisms that complement each other in anticipation of potential attack vectors.
6. Ensure user privacy protection is appropriate to the attacker model.
7. Strive for a strong enough design without hindering law enforcement agents in performing their duties should the need arise.

4. CONCLUSIONS AND FUTURE WORK

In this paper we present a domestic violence scenario where privacy is required for the protection of life. We propose a "sensible privacy" design that we argue can be achieved via usable complementary bite-size protection (suited to the user requirements as well as to the attacker model) that also mitigates misuse. In such contexts, the sensible privacy design accounts for individuals' habits and preferences and does not need to provide complete or maximal anonymity. Instead, it enables users to include technology as part of their life but be able to provide assurance against life-threatening harms that could result from privacy breach. Importantly, the sensible privacy design ensures

support for accountability to avoid misuse by perpetrators and cybercriminals.

The work presented in this paper forms part of our continuing research aimed at proposing a holistic approach to support domestic violence survivors and other vulnerable groups in accessing support services while maintaining their privacy. We cannot currently confirm with certainty that our solutions provide the sensible privacy as defined in this paper. However, we believe this approach provides a structured method to explore the problem domain. We aim to iteratively evaluate the usability and effectiveness of these solutions in controlled settings with role-play, as well as through other methodologies such as gamification.

5. ACKNOWLEDGMENTS

We would like to thank the staff at the domestic violence support centre we have been collaborating with, as well as domestic violence survivors for their time and insights that led us to carry out research in privacy issues in domestic violence scenario. The work presented here was partly supported by the UK EPSRC Research in the Wild *Hyper-privacy: Case of Domestic Violence (Hyper-DoVe)* project[1].

6. REFERENCES

[1] Greenwald, G., MacAskill, E., and Poitras, L. 2013. Edward Snowden: The Whistleblower Behind the Surveillance Revelations. *The Guardian*. 10 June 2013. Available at http://www.chebayadkard.com/uploadfile/english-article574.pdf, last accessed on 30 July 14.

[2] Boyd, D. and Ellison, N.B. 2008. Social Network Sites: Definition, History and Scholarship. *Journal of Computer-mediated communication*, 13: 210-230.

[3] Dimond, J.P., Fiesler, C., and Bruckman, A.S. 2011. Domestic violence and information communication technologies. *Interacting with Computers*, 23(5): 413-421.

[4] Emms, M., Arief, B., and van Moorsel, A. 2014. Electronic Footprints in the Sand: Technologies for Assisting Domestic Violence Survivors. *Privacy Technologies and Policy*, Springer Berlin Heidelberg: 203-214.

[5] van Moorsel, A., Emms, M., Rendall, G., and Arief, B. 2011. Digital Strategy for the Social Inclusion of Survivors of Domestic Violence. *Technical Report CS-TR-1277*, School of Computing Science, Newcastle University. September.

[6] Mansfield-Devine, S. 2009. Darknets. *Computer Fraud & Security*, 2009(12): 4-6.

[7] Hann, I., Hui, K., Lee, T. and Png, I. 2002. Online information privacy: measuring the cost-benefit trade-off. *In Procs. Int'l Conf. on Inf. Sys. (ICIS 2002)*.

[8] Raya, M., Shokri, R. and Hubaux, J. 2010. On the tradeoff between trust and privacy in wireless ad hoc networks. *In Procs. ACM Conf. on Wireless network Security (WiSec'10)*.

[9] Li, T. and Li, N. 2009. On the tradeoff between privacy and utility in data publishing. *In Procs. ACM Int'l Conf. on Knowledge Discovery and Data mining (KDD'09)*, 517-526.

[10] Crump, C. 2003. Data retention: privacy, anonymity and accountability online. Stanford Law review.

[11] Solove D. 2011. Nothing to hide: the false tradeoff between privacy and security. Yale University Press.

[12] Palen, L. and Dourish, P. 2003. Unpacking "privacy" for a networked world. *In Procs. SIGCHI Conference on Human Factors in Computing Systems,* ACM: 129-136.

[13] Nissenbaum, H. F. 2004. Privacy as Contextual Integrity. *Washington Law Review*, 79(1): 119-158.

[14] Pfitzmann, A. and Hansen, M. 2008. Anonymity, Unilinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, available at http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, v0.31, last accessed: 29 July 14.

[15] Spiekermann, S., and Cranor, L.F. 2009. Engineering Privacy. *IEEE Trans. on Soft. Eng.*, 35(1): 67-82.

[16] Goldschlag, D.M., Reed, M.G and Syverson, P.F. 1996. Hiding routing information. *Information Hiding*: 137-150.

[17] Levine, B.N. and Shields, C. 2002. Hordes: a multicast based protocol for anonymity. *J. of Comp. Sec.*, 10(3): 213-240.

[18] Reiter, M.K. and Rubin, A.D.1998. Crowds: anonymity for web transactions. *ACM Trans. on Inf. Sys. Sec.*, 1(1): 66-92.

[19] Anonymiser, http://www.anonymizer.com, last accessed 29 July 14.

[20] Dingledine, R., Mathewson, N. and Syverson, P. 2004. Tor: The second-generation onion router. In *Procs. 13th USENIX Security Symposium*, San Diego, CA, USA: 303-320.

[21] Abadi, M. 2003. Private Authentication. *Privacy Enhancing Technologies*, 2482: 27-40.

[22] Flegel, U. 2002. Pseudonymizing Unix Log Files. *Infrastructure Security,* 2437: 162-179.

[23] Kristol, D.M. 2001. Http cookies: Standards, privacy, and politics. *ACM Trans. on Internet Technology*, 1(2): 151-198.

[24] Dingledine, R., Freedman, M.J. and Molnar, D. 2000. The free haven project: Distributed anonymous storage service. *In Procs. of the Workshop on Design Issues in Anonymity and Unobservability*: 67-95.

[25] mixmaster, http://mixmaster.sourceforge.net/, last accessed 29 July 14.

[26] PGP, http://www.pgpi.org/, last accessed 16 July 13.

[27] Tails: The Amnesic Incognito Life System. https://tails.boum.org/, last accessed: 29 July 14.

[28] Logan, T. and Walker, R. 2009. Partner stalking: Psychological dominance or business as usual? *Trauma Violence Abuse*, 10(3): 247-270.

[29] Southworth, C., Finn, J., Dawson, S., Fraser, C., and Tucker, S. 2007. Intimate Partner Violence, Technology, and Stalking. *Violence Against Women*. 13(8): 842-856.

[30] Smith, G. 2013. Digital currency seized in alleged drug law violation in Charleston, *The Post and Courier*, available at http://www.postandcourier.com/article/20130707/PC16/130709585/1177/digital-currency-seized-in-alleged-drug-law-violation-in-charleston. 7 July 13, last accessed: 15 July 13.

[31] Horejsi, J. 2014. Android Forensics, Part 1: How we recovered (supposedly) erased data. Avast Blog 9 July 14. http://blog.avast.com/2014/07/09/android-foreniscs-pt-2-how-we-recovered-erased-data/, last accessed 30 July 14.

[1] http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/K012649/1