The Tragedy of the Identity Assurance Commons

Vincent Marmion, David E. Millard, Enrico H. Gerding, and Sarah V. Stevenage*
University Of Southampton
Highfield Campus
UK SO171BJ
V.Marmion@soton.co.uk

ABSTRACT

Identity assurance is the processing of personal identifying information (PII) to reach a desired confidence that an individual is who they claim to be. However, identity assurance is beyond a process; it is a commons, a natural resource accessible to all whereby individual actions can affect the group. Because each time we copy an item of PII we inadvertently expose it to misuse, which reduces the identifying utility of PII, and therefore reduces the confidence of identity assurance. Akin to the prisoner's dilemma, there is a usage dilemma in sustaining PII. A dilemma heightened by the Web as PII is being digitally exchanged, processed, and stored, with ever-increasing volume, variety and veracity.

To explore identity assurance as a commons, we develop an agent-based simulation of a simple resource strategy game. Building on work regarding the persistence of PII exploitation, our initial findings suggest that there is a potentially unsustainable dynamic in identity assurance. Therefore suggesting that in the long-term our current regulatory attempts are inapt.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**;

KEYWORDS

Identity Assurance; Personal Identifying Information; Commons

1 INTRODUCTION

Identity assurance of a person is the processing of personally identifying information (PII) to reach a desired confidence that the person is who they claim [1]. This process is integral to high-stakes activities such as the police matching fingerprints. It is also an integral part of activities on the Web, and therefore is an unavoidable and increasingly frequent part of daily life. Despite this broad and often significant application, a persistence of individual misjudgements, imposter innovations, and organisation exploitations, makes obtaining 100% confidence an unachievable goal [6]. Yet, using ever-innovative methods of extraction, i.e., biometric scanners, or a combination of methods, it is possible to get ever-closer to a person's true identity [2].

However, each process innovation has potential for negative consequences. For instance, switching from passwords to biometrics may increase assurance, but it also provokes legal, social, and ethical considerations as it enables individuals to be covertly tracked across many systems. This is because identity assurance is beyond a process; it is also a socio-technical system comprised of competing security and privacy desires, amidst commercial and social incentives, each governed by national and global regulations [5]. Moreover, identity assurance might be best considered as a commons, as the fuel of identity assurance, PII, share the same qualities as other common pool resources (CPR) [4]. Meaning, over-using PII can deplete its identifying utility in future uses, as usage involves making a copy, and each copy adds doubt as to its legitimate user. Therefore, the dilemma is in sustaining the utility of PII.

In this regard we learn from other *'tragedy of the commons'* usage dilemmas, wherein regulation is essential [3]. Insufficient regulation can allow for the accumulation of seemingly innocuous yet self-interested decisions towards the depletion of a CPR. On the other hand, simply increasing regulation can be too blunt, as overcautious protections can frustrate and waste a valuable resource. Therefore, regulation must fit.

As PII is being digitally exchanged, processed, and stored, with ever-increasing volume, variety and veracity, using ever-innovative methods of extraction, our belief is that regulation is insufficient. However, to get regulation right, first we must better understand the system. Therefore, this work builds on an existing game theoretic model to develop an agent-based simulation to study the stability and sustainability of PII within the identity assurance commons.

2 STABILITY IN THE SYSTEM

Within a game theoretical model Vila et al. [7] explores privacy akin to a second-hand car market where users pay to check for faulty cars. Likewise, the current consent model for PII disclosure costs the user in *time, effort or money* to discover whether an organisation is faulty, which in this context could be whether they extract more PII than required and/or sell it for profit. These 'faulty' organisations can capitalise on the asymmetric information between user and organisation if it is deemed that users are unwilling to pay to discover any faults. Classifying their results as a free-riding problem, they describe an oscillation between users depending on others to discover a fault, yet many individuals with this same conclusion can tempt organisations to exploit the free-riding, this in turn eventually leads to more users paying to discover while discovery exists

*Vincent Marmion; PhD Candidate of the Institute of Complex Systems Simulation.
Dr. Millard; Associate Professor of Computer and Web Science.
Dr. Gerding; Associate Professor in the Agents, Interaction and Complexity group.
Prof. Stevenage; Institute of Criminal Justice Research

WebSci '17, June 25-28, 2017, Troy, NY, USA
 978-1-4503-4896-6/17/06…$15.00
DOI: 10.1145/3091478.3098882

(Figure 1). Their results suggest the possibility of a long-term, albeit sensitive, mixed-point equilibrium comprising some attending users, others not, and some respecting organisations, others not. Therefore, exploitation persists.

Figure 1: A Privacy Free Riding Problem [7].

3 SUSTAINABILITY IN THE SYSTEM

Whilst the game-model described in [7] provides an insight into the persistence of data exploitation, the implication of the long-term sustainability of a privacy market is misleading. Because, the equilibrium is sensitive to oscillation due to environmental changes such as innovative extraction technologies. During these oscillations the asymmetry of information is heightened, leading to a higher potential of exploiting organisations, contributing to an accumulating exposure of PII over time, necessitating further innovation in the extraction of higher veracity PII. Only then, as a commons with escalating extraction and a depleting CPR, does a sustainability concern emerge.

Additional complexity is needed in order to go beyond the assumption of identical users engaging with identical organisations, and beyond a catch all of treating PII as one homogeneous entity. Repurposing [7] into an agent-based model provides the flexibility to add these elements, and also add realism to the insights gained.

4 A NEW AGENT-BASED MODEL

The following simple outline of an agent-based version of [7] describes two service agents competing for the engagement of a population [P] of user agents. The service perspective amounts to a 2-player, iterated, pure strategy game. Each service selects either a respect [R] or an exploit [E] strategy. They have knowledge of their opponents current strategy, and a basic calculation of predicted market change. Profit is calculated per number of users (u) as $eu = ru + u\epsilon$. The user perspective equates to a simple decision problem, whereby in each turn [T] a random set of users (1-4%) evaluate their position; ignoring users join, or remain engaged with, any service, attending users join or remain with a respecting service, and leave or remain disengaged from an exploiting service.

Figure 2 illustrates the results of this, *in essence*, agent-based simulation of [7]. The top and middle panels indicate the oscillations as described in Figure 1 with exploitation coinciding with cycles in market latency, i.e. disengaged users. The middle panel showing user reaction to exploitation reflects what Westin [8, p. 24] describes as a 'shift in public mood', during 1999 and 2002 as 'privacy fundamentalists' rose from 24% to 34%. Not shown here, is the model sensitivity to changes in ϵ, as slight decreases reduce the oscillations in favour of stable respect strategies, whereas slight increases causes exploitation strategies to dominate.

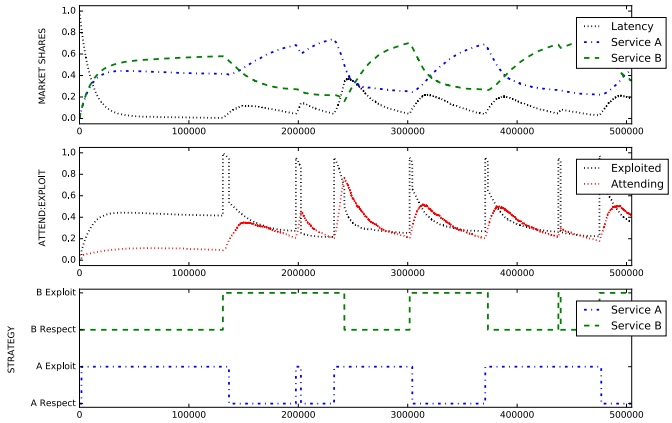

Figure 2: *Top:* Market shares, and latency. *Middle:* Periods of exploitation and the reactive user attend strategies. *Bottom:* Oscillation of dominant strategies as size changes reach tipping points. *Parameters:* $r = 1, \epsilon = 0.005, P = 15000, T = 3000$

5 CONCLUSION AND FUTURE WORK

This abstract sets out an argument for examining identity assurance as a commons. Building on this premise could have significant implications for the regulation of identity assurance, and specifically, for how we regulate for the sustainable use of PII in a digital age. It also illustrates the first development steps of an agent-based simulation of the identity assurance commons. This approach provides a flexible base from which to explore different aspects of the Identity assurance commons, including what drives or tempers usage escalations in identity assurance. To this end, two sets of empirical studies are underway to enrich this model. The first exploring the different ways users make disclosure decisions, i.e., calculative vs heuristic, and a second examining how users personally value individual items of PII.

REFERENCES

[1] Yolanta Beres, Adrian Baldwin, Marco Casassa Mont, and Simon Shiu. 2007. On identity assurance in the presence of federated identity management systems. In *Proceedings of the 2007 ACM workshop on Digital identity management - DIM '07*. ACM Press, New York, New York, USA, 27.

[2] Sue M Black, Sadie Creese, Richard M Guest, Bill Pike, Steve J Saxby, Danaë Stanton Fraser, Sarah V Stevenage, Monica T Whitty, Danae Stanton Fraser, Sarah V Stevenage, and M T Whittty. 2012. Superidentity: Fusion of identity across real and cyber domains. *ID360: Global Identity* (2012).

[3] Garrett Hardin. 2009. The Tragedy of the Commons. *Journal of Natural Resources Policy Research* 1, 3 (2009), 243–253.

[4] Charlotte Hess and Elinor Ostrom. 2003. Ideas, artifacts, and facilities: information as a common-pool resource. *Law and contemporary problems* 66, 1/2 (2003), 111–145.

[5] Daniel J. Solove. 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review* 44, May (2007), 1–23. DOI: https://doi.org/10.2139/ssrn.998565

[6] Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil K. Jain. 2004. Biometric cryptosystems: Issues and challenges. *Proc. IEEE* 92, 6 (2004), 948–959. DOI: https://doi.org/10.1109/JPROC.2004.827372

[7] Tony Vila, Rachel Greenstadt, and David Molnar. 2003. Why we can't be bothered to read privacy policies models of privacy economics as a lemons market. In *Proceeding ICEC '03 Proceedings of the 5th International Conference on Electronic Commerce*. ACM, 403–407. DOI: https://doi.org/10.1145/948005.948057

[8] Alan F Westin. 2003. Social and political dimensions of privacy. *Journal of social issues* 59, 2 (2003), 431–453.