7-12-2021

Digital Identities – Impact of Information Privacy Awareness on Identity Threats

Nidhi Tewari
University of Canterbury, nidhi.tewari@pg.canterbury.ac.nz

Annette Mills
University of Canterbury, annette.mills@canterbury.ac.nz

Digital Identities – Impact of Information Privacy Awareness on Identity Threats

Submission Type: Research-in-Progress

Nidhi Tewari
University of Canterbury
Christchurch, New Zealand
nidhi.tewari@pg.canterbury.ac.nz

Annette Mills
University of Canterbury
Christchurch, New Zealand
annette.mills@canterbury.ac.nz

Abstract

Identities help individuals understand who they are and are a tool to project themselves before others in ways they desire. This is achieved through privacy, which provides control over information sharing. However, complexities arise with digitalization of information and creation of digital identities. Digital identities are highly malleable and entities (whether human/non-human) other than the data subject themselves can add, delete, and modify information about others leading to loss of privacy and increasing privacy concerns and identity threats. Identity threats are met with responses from individuals and can potentially impact society negatively. At the same time, there are legislative frameworks that aim to protect individuals' privacy rights. While there is research linking identity and privacy, the role of privacy concerns in the formation of identity threats and impact of awareness of protective mechanisms has had little attention. This study addresses his gap by exploring the relationship between privacy concerns, information privacy awareness (of legislative frameworks) and identity threats in the context of digital identities.

Keywords: *Identity, Information Privacy, Identity Threats, Information Privacy Awareness*

Introduction

> *On Saturday, 13 February 2021, climate change activist, 22-year-old Disha Ravi, was arrested for her involvement in the farmers' protests in Bengaluru, India. These protests have been going on since 2020 to oppose three farm bills passed by the parliament of India. Ravi was charged with sedition, criminal conspiracy and inciting unrest, her crimes related to a 'toolkit' document that sets out strategies to support the protests, which the police claimed as evidence of a coordinated international conspiracy against India. But before the court of law could evaluate the charges, social media declared her guilty and added false claims about her religion and being a single mother, which went viral (The Quint, 2021[1]).*

People have an inherent need to control and regulate others' perceptions of them. This is primarily to gain acceptance, appreciation and approval, and escape being shunned by society. They do so by creating various social identities (e.g., as a sibling, a friend, or a basketball coach for under 15s) and using privacy as a tool, to regulate the information that each of these identities comprise of. As such, information that one may reveal to family or friends will differ from what is disclosed in the workplace. While there are overlaps between identities (i.e., some information will be common), they are distinguished by varying what is known about a person or attached to their identity in each context.

[1] Available at https://www.thequint.com/news/webqoof/disha-ravi-is-not-a-christian-or-a-single-mother-fact-check

However, advances in information technology particularly in the use of the internet and social media (Poushter et. al., 2018) have significantly increased the extent to which our identities are digitalised, and in some cases, made public. With these changes it is increasingly important for individuals to have control over how they are represented in the digital space (Rettberg, 2009). This can influence them both in the digital and in the physical world, including the information they see, the services, products, and opportunities they are offered or have access to, and their relationships with others. The impacts can be significant, as the case of Disha Ravi illustrates. Although some news agencies and social media handlers were willing to publish information to rectify the false claims made again Disha Ravi, without some way of being able to regulate privacy, what and how information is used, as individuals we may have little control over our identities and how we are presented in the world around us. This is especially challenging when the digital space is a key source of information about us, and anyone (i.e., organisations, friends, family and, strangers) can add information that modifies our identity, changes how we are seen by others, and impacts our reputation. Social media is particularly challenging as information, whether true or false, can spread at such a pace that it can have significant impacts within minutes, not only on the data subjects themselves but also on the wider society and on organisations (Aral et al., 2019; Figueira & Oliviera, 2017). Subsequently, concerns about privacy arise as individuals feel they are losing control over their information and by extension their identity; this leads to the emergence of threatened identities. Such threats in turn, can lead to undesirable outcomes such as discrimination, misinterpretation, and misrepresentation, and trigger responses from the individuals themselves, such as taking action to conceal their information or discrediting the source of that information (Petriglieri, 2011).

While there are studies which show that there is a relationship between privacy and identity (Petronio 2002; 2015), and which trace the formation of identity threats through loss of control over one's information, there is no substantial work which links emergence of information privacy concerns to identity threats. Such work is of contemporary importance given that digitalised information is difficult to control, regulate and manage, and digital identities are taking over how social identities are represented.

To address privacy concerns, there are legislative frameworks that provide for the protection of privacy such as the General Data Protection Rule (GDPR, 2018) and OECD Privacy Guidelines (2013) at the international level, and the FTC Principles (USA) and New Zealand Privacy Act (2020) at the domestic level. These legislative frameworks provide for privacy protection mechanisms that may increase the awareness of such protective mechanisms and reduce identity threats. However, research on the impact of privacy assurance through mechanisms such as legislative frameworks is limited. Where examined, studies show many users are not aware of the mechanisms available to help them manage their privacy online, and where there is knowledge, this does not necessarily lead or empower them to take action to control their privacy (Smit et al., 2011; Strycharz et al., 2021). Given the gaps in current research and increasing importance of digital identities, this study aims to address the following research question:

What is the impact of privacy concerns and of awareness of privacy protective mechanisms (in the form of legislative frameworks) on the formation of identity threats in the context of digital identities?

Literature Review

Prior research suggests a relationship between identity and privacy (Petronio 2002; 2015) so theoretically, a relationship can be inferred between privacy concerns and identity threats. Indeed, privacy and identity are so interwoven that some scholars believe that one's informational sphere and one's personal identity are two sides of the same coin (Floridi, 2006). To understand this concept further, the following review explores in brief, key concepts, and prior research on privacy (particularly information privacy), identity and identity threats.

Identity

Individuals value their identity as it not only aids them in connecting to their actual selves, but it also facilitates their relationships with others. Research recognizes two distinct yet related aspects to one's

identity – (i) self-identity i.e., people's conceptions of who they are, of what sort of people they are, and how they relate to others (Abrams and Hogg, 1988) and (ii) social identities i.e., that part of one's identity that derives from membership in a group or social category (Brewer and Gardner, 1996). While individuals will have a single 'identity' that is regarded as the 'self-identity', they will have multiple social identities, each of which is situation- and/or role-specific (e.g., as a parent, a child, an employee, a customer). Social identifies are distinguished through people being able to exercise control over what information is shared in relation to each identity and the associated relationship (e.g., family vs. workplace relationships, parent vs. child). This enables differentiation of one social group (or role) from another and the proper functioning of a person within that group/role (e.g., as a parent within their family context vs. employee or manager in the workplace).

The preservation and protection of one's identities is critical for the psychological and emotional well-being of individuals and when people realize that others can find information about them which is false or which they did not provide and/or did not want to disclose, it has a psychological impact (Abelson et. al., 1998). While some information can lead to positive consequences such as promotions (even if the information is false), some information can lead to serious negative consequences such as reputational and lifestyle damage, depression, physical violence, and suicide. This indicates the manifested need of people to be able to control and regulate their social identities - this is where privacy comes into the picture. Privacy is perceived as a tool for exerting control over one's personal information (Allen, 1999) which can enable individuals to decide what information they want to share with others and how. With the increasing use of digital platforms such as social media websites, e-commerce, and various information systems, our identities are becoming increasingly digitalized, leading to emergence of the digital identity.

The 'digital identity' (also referred to as an 'informational identity') is a subset of one's identity, comprised only of information that is digitalized – digital identities are therefore partial compared to the underlying personal or social identity. As individuals, we create digital identities for ourselves as users of digital platforms (Majeed, Adisaputera and Ridwan, 2020). Hence, one definition of a digital identity is a set of claims made by one digital subject about itself or another digital subject (Cameron, 2005), where the term 'digital subject' refers to 'a person or thing represented in the digital realm which is being described or dealt with'. Williams et. al. (2010) views the term 'digital identity' as describing the persona that a person projects across the internet and it is, therefore, a reflection of others' perception of them based upon the information they provide about themselves and the information that others provide about them. Taken altogether, a digital identity represents the sum of the information about an individual available in a digitalized form (Bozkurt, 2016). Digital identities, being sub-sets of one's identity, are also multiple (based on different social contexts and roles) which draw on various subsets of information associated with a person (but are not limited to) including general information (e.g., name, age, gender, marital status as relevant), health information, travel information, financial information, etc. (Clauβ et. al., 2005).

Like the core notion of identity, digital identities are significant to individuals as these reflect facts about them and gives an insight into how they want to be perceived (or are perceived) in their social environment. These identities integrate various sources of personal information, reflect private thoughts and social behaviors, and contain facial images, etc. These contain information about the individual (Bozkurt, 2016; see also Ambady and Skowronski, 2008; Hall and Berneiri, 2001; Vazire and Gosling, 2004) whether this was provided by the individual themselves or by others (whether human or non-human entities) and whether they are 'original facts' or derived from patterns based on the individual themselves and/or others. Digital identities are therefore significantly malleable as entities (human/non-human), other than the individual themselves, can delete/modify information about them (Papaioannou et. al., 2019), which leads to significant concerns. These include loss of ownership and control over the digital identity (Ayed, 2011), profiling and drawing inferences whether accurate or inaccurate, and negative consequences such as discrimination and uncovering undisclosed information (Peppet, 2014). The rise of information privacy concerns therefore reflects the importance individuals (as users) place on wanting to control how they are perceived across digital platforms. This control, however, can only

be actualized when the individuals are the ones in-charge of adding or modifying information about themselves; however, this is not the case.

In the absence of digital domains and platforms, individuals previously had more control over their identities. They could regulate how they portrayed themselves in a society as they had more control over how and with whom information was shared. However, with digital identities, the control individuals have over how others see them has loosened and hence, there are certain concerns which arise from the evolution and use of digital identities. Such concerns, in turn, can lead to the formation of identity threats.

Identity Threats

An identity threat is any thought, feeling, action or experience that challenges an individual's personal or social identity (Breakwell, 1983). Since digital identities are a part of the social identity of an individual, lack of control over one's digital identity can lead to identity threats, which in the context of the digital identity may be further conceptualized as *an expectation of harm to an individual's self-belief* b*rought about by the use of digital identities* (Craig, Thatcher and Grover, 2019). Identity threats may either harm the identity in the present (Breakwell, 1983) or have a potential harm in the future (Lazarus and Folkman, 1984). The identity threats can also devalue the identity of an individual (Petriglieri, 2011), i.e., the self-worth derived from holding that threatened identity is reduced (Ashworth et. al., 2007; Petriglieri, 2011). Since their identities determine their sense of self-worth (Gecas, 1982), individuals take identity threats seriously, and will address them by engaging in identity-protecting responses (Craig, Thatcher, and Grover, 2019; Petriglieri, 2011) through regulating one's privacy.

Privacy and Identity

Pastalan (1970) defines privacy as the right of the individual to decide what information about themselves should be communicated to others and under what conditions. The foremost reason why people value privacy is that one's informational sphere and one's personal identity are considered as two sides of the same coin (Floridi, 2006). Privacy enables individuals to create and maintain their image in given social spaces, which varies with the social spaces. Westin's perception that privacy includes control and freedom to make a choice about the disclosure of information has been supported by Rapoport (1972) who defines privacy as the ability to control interaction, to have options, devices and mechanisms to prevent unwanted interaction and to achieve desired interaction. Similarly, Proshansky et al. (1970) state that privacy is obtaining freedom of choice or options to achieve goals, control over what, how and to whom a person communicates information about the self. Together, these definitions reflect the underlying view that privacy is a means of regulating one's social identity and it enables individuals to create and preserve their self-identities without external interference.

Information privacy is a subset of privacy where the subject matter is information in a digital form. Information privacy exists also because there is a desire to protect information. Information privacy is extremely valuable because it acts like a shield for one's personal identity (Floridi, 2006). The early views on information privacy suggest it is a set of concerns that include what kind of information can be disclosed, what kind of information cannot be disclosed, when can an individual not be forced to disclose certain information and what safeguards are available (Mason, 1986). A more recent view is that "information privacy refers to the desire of the individuals to control or have influence over some data about themselves" (Belanger and Crossler, 2011).

Information Systems research typically views information privacy as a concept, which includes concerns, interests, and functions. It further recognizes that such concerns and interests are dynamic in nature. The basic premise, that information privacy is a set of concerns, rests on the assumption that there is information that requires protection. Two noteworthy representations of information privacy are captured in: (i) the Concern for Information Privacy Model given by Smith el al. (1996) which identifies four main privacy concerns namely, collection, unauthorized secondary use (internal and

external), improper access and, errors; and (ii) the Internet Users' Privacy Concerns Model given by Malhotra et al. (2004) which focuses on collection, control, and awareness of privacy practices.

Research Framework

The relationship between identity and privacy is not easy to define. However, there are macro level frameworks like Communication Privacy Management (CPM) Theory that provide insights. CPM Theory (Petronio, 2002) explains the relationship between identity and privacy through the concept of ownership. The basic premise of the CPM theory is that individuals value their identity and as a result, they want to exercise ownership over their data. Loss of ownership over their data, leads to the formation of privacy concerns and that, in turn, has a negative impact on privacy attitude. However, absolute ownership over a data object ends as soon as it is shared; this is a key reason why privacy concerns emerge when information is shared.

Protection of identity, hence, serves as a motivation for individuals to exercise ownership over their data (Petronio and Child, 2020) and to exercise that ownership individuals create boundaries. These boundaries (comparable to a semi-permeable membrane) allow the flow of information from one stakeholder to another and open/close at the behest of the stakeholder who owns the information. Privacy rules are formed by the stakeholder themselves, to ensure that their interests are protected i.e., they reveal what they want to reveal to others, which forms the basic premises of social identities (Fearon, 1999) and conceal what information they want to keep to themselves, which reflects the protection of self-identities (Hall, 1989). However, once the information is shared, that is, the data object is transferred from one entity (i.e., the transferor) to another (i.e., the transferee), the transferor loses absolute ownership and cannot regulate how the other stakeholder subsequently uses that information. Moreover, even if the transferor does not share personal information or actively conceals information, with advances in big data, analytics, and AI Systems, non-personal information can be used to infer personal information or information provided can be used to infer information that was concealed (Janecek, 2018). As such, the loss of ownership over information can lead to the formation of privacy concerns.

Information Privacy Awareness and Identity Threats

The success of legislative policies such as the GDPR depends on: (i) the individual's awareness of their information privacy rights, and (ii) how they act upon those rights (Correia and Compeau, 2017). When individuals are not aware of their rights, they cannot be expected to take suitable actions to preserve their information privacy. Unfortunately, it is practically impossible to be fully aware of matters, such as, whether others have received personal information about one's activities, who they are, and what personal information they have received (Potzsch, 2008). Indeed, the digital sphere is too wide for an individual to keep track of information related to themselves. Hence, what is required is not awareness of the possibility of loss, but the awareness of how the loss can be prevented and what are the available remedies (e.g., legal recourse) when the loss occurs.

Since a digital identity is a sub-set of one's identity, threats to the digital identity, whether perceived or actual, also threaten the identity of the individual. Drawing on the above discussion and supported by the Identity Threat Framework (Petriglieri, 2011; see also Craig, et al., 2019) and the Antecedent, Privacy Concerns and Outcome Model (Smith et al., 2011), this study proposes that when digital identities are formed and absolute ownership over one's information is lost, this leads to the formation of privacy concerns and identity threats as an outcome of those privacy concerns. It further proposes that increased information privacy awareness will reduce identity threats. Taken together (See Figure 1), this study examines the following hypotheses:

H1: Privacy concerns is positively related to identity threats
H2: Information privacy awareness is inversely related to identity threats

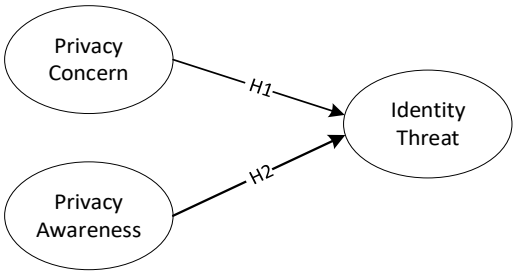

Fig. 1 Research Framework

Research Method

To assess the research model (Figure 1), a two-phase study supported by interviews and document analysis, followed by a survey will be conducted. For this study, conceptualization of information privacy awareness will focus on awareness of legislative frameworks (such as the GDPR). Measures for privacy concerns, which arise from the creation and use of digital identities, will be adapted from interview findings, the literature, and existing scales (e.g., Malhotra et. al., 2004; Smith et. al., 1996). These privacy concerns are regarded as the threat source and may include (but are not necessarily be limited to) concerns around consent (i.e., collection and subsequent use of information), reasonability of use, and errors. Survey data will be analyzed using structural equation modeling (SEM). As the aim is to determine the likelihood and extent of identity threat formation inferred from privacy concerns and information privacy awareness, a path modeling approach to structural equation modeling (SEM) is appropriate (Hair et al., 2016).

Proposed Contributions and Conclusion

Prior research suggests that privacy and identity go together (Floridi, 2006), hence it is expected that concerns about privacy will lead to identity threats. However, there is limited empirical work examining the role of privacy concerns, and how identity threats might be minimized. Increasing use of digital identities and reliance on them for decision-making are also reasons for seeking to understand how loss of control over digitalized information impacts identities, and lead to identity threat.

To address this gap, this research examines the role of privacy concerns in the formation of identity threats. It also aims to explore whether and to what extent would awareness of legislative frameworks (or the fact that individuals have privacy rights and a recourse if those rights are breached) aid in reduction of identity threats. Additionally, the study may also be able to identify whether individuals believe that legislative frameworks can protect their interests and provide remedies. The results are expected to shed light on the relationship between privacy and identity contributing to and extending the current understanding of the role of privacy in the context of digital identity management and its impact on identity threat formation. It is also expected to provide insights leading to further research on enhancing the protection, regulation, and management of digital identities (by identifying loopholes in legislative frameworks, if any) in a way that minimizes identity threats and maximize protection of the interests of individuals in relation to their identities. This study is therefore an attempt to bring together the disciplines of information systems, law, and policy to understand how information privacy can be used efficiently as a tool to protect the inherent right of individuals to have control over their identities.

References

Abelson, H., Lessig, L., Covell, P., Gordon, S., Hochberger, A., & Kovacs, J. 1998. "Digital identity in cyberspace," *White Paper Submitted for 6.805/Law of Cyberspace: Social Protocols*.

Abrams, D., & Hogg, M. A. 1988. "Comments on the motivational status of self-esteem in social identity and intergroup discrimination," *European journal of social psychology*, *18*(4), 317-334.

Allen, A. L. (1999). "Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm," *Conn. L. Rev., 32*, 861.

Ambady, N., & Skowronski, J. J. (Eds.). 2008. *First impressions*. Guilford Press.

Aral, S., & Eckles, D. 2019. "Protecting elections from social media manipulation," *Science, 365*(6456), 858-861.

Ashworth, G. J., Graham, B., & Tunbridge, J. E. (2007). Pluralizing pasts. *Heritage, identity and place in multicultural societies*.

Ayed, G. B. 2011. "Digital identity metadata scheme: A technical approach to reduce digital identity risks," *2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications* IEEE. pp. 607-612).

Baier, T., Zirpins, C., & Lamersdorf, W. 2003. "Digital identity: How to be someone on the net," *Proceedings of the IADIS International Conference of e-Society* (Vol. 2) pp. 815-820.

Bélanger, F., & Crossler, R. E. 2011. "Privacy in the digital age: a review of information privacy research in information systems," *MIS quarterly*, pp.1017-1041.

Bozkurt, A., & Tu, C. H. 2016. "Digital identity formation: Socially being real and present on digital networks,) *Educational Media International, 53*(3), pp. 153-167.

Breakwell, G. M. 1983. *Threatened identities*. Wiley.

Brewer, M. B., & Gardner, W. 1996. "Who is this" We"? Levels of collective identity and self-representations," *Journal of personality and social psychology, 71*(1), pp. 83.

Cameron, K. 2005. "The laws of identity," *Microsoft Corp, 12*, pp. 8-11.

Clauβ, S., Kesdogan, D., & Kölsch, T. 2005. "Privacy enhancing identity management: protection against re-identification and profiling," *Proceedings of the 2005 workshop on Digital identity management*. pp. 84-93.

Correia, J., & Compeau, D. 2017. "Information privacy awareness (IPA): a review of the use, definition and measurement of IPA," *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Craig, K., Thatcher, J. B., & Grover, V. (2019). The IT Identity Threat: A Conceptual Definition and Operational Measure. *Journal of Management Information Systems, 36*(1), 259-288.

Fearon, J. D. 1999. "What is identity (as we now use the word)," *Unpublished manuscript, Stanford University, Stanford, Calif.*

Figueira, Á., & Oliveira, L. 2017. "The current state of fake news: challenges and opportunities," *Procedia Computer Science* (121), pp.817-825.

Floridi, L. 2006. "Four challenges for a theory of informational privacy," *Ethics and Information technology* (8:3), pp. 109-119.

Gecas, V. 1982. "The self-concept," *Annual review of sociology* (*8*:1), pp. 1-33.

Ginger, J. 2008. "The Facebook project-Performance and construction of digital identity

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage publications.

Hall, D.T. (2000) *Careers in and out of organisations.* Thousand Oaks, CA: Sage.

Hall, J. A., & Bernieri, F. J. (Eds.). 2001. *Interpersonal sensitivity: Theory and measurement*. Psychology Press.

Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer law & security review, 34*(5), 1039-1052.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer publishing company.

Majeed, M. M. F., Adisaputera, A., & Ridwan, M. 2020. "Digital Identity," *Konfrontasi: Jurnal Kultural, Ekonomi Dan Perubahan Sosial*. (*7*:4), pp. 246-252.

Malhotra, N. K., Kim, S. S., & Agarwal, J. 2004. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information systems research*. (*15*:4), pp. 336-355.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS quarterly*, 5-12.

Papaioannou, T., Tsohou, A., & Karyda, M. 2019. "Shaping digital identities in social networks: Data elements and the role of privacy concerns," *Computer security*. Springer, Cham. pp. 159-180.

Pastalan, L.A. (1970). Privacy as a behavioral concept. Social Sciences, 93-97.

Peppet, S. R. 2014. "Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent," *Tex. L. Rev* (*93)*, pp. 85.

Petriglieri, J. L. 2011. "Under threat: Responses to and the consequences of threats to individuals' identities," *Academy of Management Review* (*36*:4), pp. 641-662.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. SUNY Press.

Petronio, S. 2015. "Communication privacy management theory," *The international encyclopedia of interpersonal communication*. pp. 1-9.

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: utility of communication privacy management theory. *Current Opinion in Psychology*, *31*, 76-82.

Pötzsch, S. 2008. "Privacy awareness: A means to solve the privacy paradox?," *IFIP Summer School on the Future of Identity in the Information Society*. Springer, Berlin, Heidelberg. pp. 226-236

Poushter, J., Bishop, C., & Chwe, H. 2018. "Social media use continues to rise in developing countries but plateaus across developed ones" *Pew research center* (*22)*, pp. 2-19.

Proshansky, H. M., Ittelson, W. H., & Rivlin, L. G. (Eds.). 1970. *Environmental psychology: Man and his physical setting*. New York: Holt, Rinehart and Winston. pp. 21-26.

Rapoport, A. (1972). *Some perspectives on human use and organization of space*.

Rettberg, J. W. 2009. '" 'Freshly Generated for You, and Barack Obama' How Social Media Represent Your Life," *European Journal of Communication* (*24*:4), pp. 451-466.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly, 167-196.

Strycharz, J., Smit, E., Helberger, N., & van Noort, G. (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior*, *120*, 106750.

Vazire, S., & Gosling, S. D. 2004. "e-Perceptions: Personality impressions based on personal websites," *Journal of personality and social psychology* (*87*:1), pp. 123.

Williams, S. A., Fleming, S. C., Lundqvist, K. O., & Parslow, P. N. 2010. "Understanding your digital identity," *Learning Exchange* (1:1).