Social Network Culture Needs the Lens of Critical Trust Research

Natasha Dwyer, Stephen Marsh

Social Network Culture Needs the Lens of Critical Trust Research

Natasha Dwyer[1], Stephen Marsh[2],
[1] Victoria University,Melbourne, Australia
natasha.dwyer@vu.edu.au
[2] University of Ontario Institute of Technology, Oshawa, Canada
stephen.marsh@uoit.ca

Abstract. Trust is essential to the success of the social networks that are aggregating and applying masses of information about us. In this position paper, we argue that a critical approach to exploring trust and social networks is required; this entails genuinely working in the interests of users and acknowledging the power relations and wider social context of this form of technology that is impacting more and more of our everyday life. Without a critical approach, digital environments may become monopolised by corporate interests.

1 Introduction

The digital traces left by individuals can now easily be collected, crosschecked and stored as part of a phenomenon known as social networking and what is loosely described as 'big data'. Because this complex set of information can be used as a form of social control, social science researchers argue that we need to handle social network data and culture critically; to question the ways the data is gathered and used and to produce alternative means to understand and participate in the phenomenon [1]. But what does this mean for trust researchers? In this position paper, we contend that critical approaches to trust and social networks require researchers to work *genuinely* in the interests of users and to respond to the power relations connected with social networks. We suggest that trust researchers should follow the lead provided by privacy researchers, in acknowledging that the interests of an individual can clash with those of governments and corporations. Before we outlay our argument, we describe what social network data is and explain the central role trust plays in the success of the social networks that produce the data. As a final point, we discuss how social network data can be of use to trust researchers.

2 Social Network Data

Social network data is generally considered to be information generated at networks designed for exchange between users, for example, messages exchanged at websites such as Twitter and Facebook. Social network content has existed in some form for

some time. More recently, content collected from disparate locations can be united, compared and stored at a magnitude not previously possible. The digital data provided by individuals can be analysed and applied in a variety of ways. For instance, social network users, such as subscribers to Facebook, now receive advertisements for products their friends have bought: the underlying idea behind the strategy is that individuals trust the recommendations of their friends so the technique is an effective way to convince users to buy a product or accept a message. Social network analysis, used by industry and the academy, explores the links between individuals, behavior and artifacts (for instance, messages) to find patterns, such as the flows of information and influence.

A social network occurs when a computer connects individuals or organizations, according to Garton [2], so the data could include material as diverse as logs indicating which individuals share a printer to transcripts of credit card transactions. Self-tracking systems, applications that gather data about individuals' health performance also now need to be considered as a type of social network content. Systems are now available that enable individuals to track and compare their personal health indicators such as eating habits, sleep, blood pressure etc. There is the option to share this information with others via broadcasts on social networks. Daly [3] outlines how although these systems were once the domain of a few 'enthusiasts', interested in the response of their bodies of the course of a day, the information is now in the hands of multinationals who are beyond the reach of local laws describing how personal information should be protected. Another ramification of self-tracking technology is that now, according to Lupton [4], individuals are not trusting their own insights about their bodies and health because it's easier to trust the 'numbers over physical sensations'. Self-tracking systems teach us to adhere to expected societal norms regarding sleeping, eating, and drinking, which are reinforced through the act of sharing data. One aim of these systems is to use personal data as a form of motivation to improve one's health through self-reflection, guilt and peer pressure [4]. Soon employers may demand access to their employees' health information and decide on who is trustworthy on the basis of these results [5].

3 Social Networks and Trust

Trust plays a central role in the continuing flow of social network content to adapt Fukuyama's famous line [6], trust greases the wheels of the networks. If a user does not trust the information received from a network, it will not be passed on [7]. The business model of the social network sites depends on users creating, sharing and consuming content. IBM's CEO, Ginni Rometty in 2014 described the opportunity for the sale of individual private data as the goldmine for the 21st century [8]. So social network sites are designed to provoke high levels of disclosure from users. For instance, participation can be set up in a popularity contest framework where users strive to receive more attention in the form of 'likes' and 'shares' etc. [9]. The website 'Dark Patterns' (www.darkpatterns.org) is a collection of instances where the designer has applied a solid understanding of human nature in order to coerce the user into doing something that is not in the user's individual interest, for instance,

disclosing personal information. An example provided by Dark Patterns is Yahoo's Hotjob site. In order to interact, the user is required to answer a series of personal information, even though the information required by a potential hirer is already provided in the job application. As the user is required to complete the information fields in order to progress an application, there is pressure to comply.

The uneven power relations propagated by social networks means that individuals can be manipulated and controlled, whether by marketing companies, governments, or any other entity that has access to the data and the means to analyse it. This is known as 'information injustice'. Individuals are often unaware of the data traces they are leaving and the value of the information they leave behind [10], as demonstrated by the disturbing effect of the viral website 'Take This Lollipop' (www.takethislollipop.com). Upon entry to this site, the user is asked to provide permission for an app to access the user's personal Facebook account. This is a common request from many websites, so users are accustomed to agreeing without much consideration. Once permission is granted, there is a film sequence of a grimy house with a menacing looking man typing on computer. The camera moves closer and we see what he is looking at. Integrated into the film image is the personal Facebook profile view of the user that contains information that the user has not yet set to public display. This includes information that the user may not have given directly to Facebook, such as birth date, that Facebook has collected from one of its partner organisations. The intention of 'Take This Lollipop' is to shock. Even if an individual is alert to the circulation of personal data via a social network, it is difficult for an individual to retract a data trace once it is distributed [10]. The exploitation of users is built into the design of technology, as price for use. When someone uses technology to conduct some sort of activity, such as a searching, buying products, or catching up with friends, the user enters into an arrangement where personal data is collected as a condition of use of the technology [11].

As trust plays a central role in the creation of successful social networks, it is easy to see how the work of trust researchers is attractive to owners of digital environments such as corporations and governments. Trust research can be used to exploit users and to create environments that are commercially successful by giving the appearance of trustworthiness. If trust researchers take their work seriously and believe it has an impact on the direction of both the research field and industry, then an implication is that the work could be used to improve the profits and control of a private company. For instance, [12] study trust interactions on social network sites from a user's perspective, in particular, how a user can improve social capital in these environments. They recommend that as well as having many 'loose ties' users should stay visible in these spaces and remain attentive to their contacts. Social networks such as Twitter and Facebook could use this advice to encourage users to keep engaging with their systems. Similarly, Lui et al [13], working with the notion that different users in a social network seek a range of trust evidence, seek a means to calculate tailored trust ratings, which they refer to as Quality of Trust. However, a social network developer could use this research to persuade users to buy the products they endorse. There may be researchers who may be comfortable with their work servicing the support of the status quo. However, for those researchers are not, we argue that a critical approach is required. Of course, as Gupta [14] points out, it is

possible that any idea and critique can be subsumed by the mainstream to maintain the current state of affairs, but this does not mean that resistance is useless.

There are other roles that trust research can play and one importance stance is to work in the interests of users first, not commerce. To argue for a critical approach to technology is not to declare the technology as dystopic. Rather it is to understand technology as a 'double-edged sword' reliant on 'the context and comportment' of a particular scenario including the actions of and interplay between digital environment owners, developers, designers, and users [15].

4 A Critical Approach to Trust and Social Networks

So what does a critical approach to studying and designing trust consist of? A critical perspective entails two key actions by researchers that are reviewed in this section. Firstly, an acknowledgement is required of the power relations inherent in the domain of social network data, trust and research. Acknowledgement entails questioning whose biases and expectations are served by the production of digital systems and the research that surrounds digital technology [16]. Acknowledgement can lead to research and design that deciphers technology as a social construct that enables a range of social relations not just those that suit governments and corporations [17]. (Alternatively, acknowledgement of the power relations can lead to the researcher identifying that there is limited possibility for research with a critical perspective, a discussion beyond the scope of this paper).

However, according to Stolterman [18], scientists and engineers are not well-suited to undertake a consideration of the socio-political framework their work exists in. They are unaccustomed to such a practice as their training involves focusing on one problem and isolating it away from context much as possible. Zelenko and Felton [16] add that designers are also not well suited to consideration of the wider milieu that their work exists in as they are trained to acquiesce to the instructions of the client. But education and practice is changing. The trust research field, including practitioners from a range of disciplines, now conceptualise trust as a social phenomenon. The next step is to move beyond conceptualising trust as a scenario between individuals or groups and consider the wider social and political structures impacting on individual interactions. An example of research that includes a consideration of social context is the work of Pearson and Tsiavos [19] who explore 'smart notices'; a means for individuals to control their information and to set the expectations for the products and services they seek. Although they are working in a corporate environment (HP Bristol), these authors place their research in a socio-technical context, the Creative Commons movement, and design around the inherent power relations that occur between an individual and a network.

Secondly, researchers need to commit to working *genuinely* in users' interests; addressing information imbalances, making users aware of their trust interactions, enabling users to negotiate trust on their own terms and learning from users. Trust researchers can learn from privacy researchers who have a natural inclination to study a scenario from the perspective of users' welfare. As Krontiris [20] review, privacy research has a long history of conceptualisation as tussle between an individual and

others who might gain advantage from private knowledge about that individual. Some protection for individuals is legislated and there is also a long history of privacy advocacy that provides a framework that researchers' work can fit into. Some privacy researchers explore the risks that users are exposing themselves to by interacting with social networks. For instance, Nurse et al [21] investigate the hazards from the occurrence of incidental individual interactions online. Some actions are as innocuous as printing from a device. A mass of data is left behind that can be used to infer about that individual's 'real world social relationships', without the individual having any knowledge of the disclosure. Those inferences could be used in a myriad of ways depending on who had access to the data. Netter et al [22] add that there is often a mismatch between a user's perception of privacy controls in a social network and what is really occurring. To solve this problem, they have developed identity management software to assist a user to handle disclosures made online. Basu et al [23] suggest a system that could work without the disclosures and privacy trade-offs users are accustomed to offering in order to participate. Games are becoming a location for mass amounts of social network data, as players reveal physiological and psychological data (for instance, response time, prioritisation of strategies and attention rate) and Martinovic et al [24] argue that this is an area that needs attention from privacy researchers.

Readdressing information imbalance is to strive so that individuals have as much access and control to the data generated by networks as do powerful bodies such as governments and private corporations. Mann [25] is a proponent of this technique. His response to surveillance is 'sousveillance', that he defines as 'the recording of an activity by a participant in the activity' to 'reverse the otherwise one-sided panoptic gaze'. In this vision, individual users adopt the recording technologies in the spaces they inhabit and combine their resources to form lobby groups. We see these types of community groups already happening in the form of police observation groups such as *Copwatch* in Canada and *FITwatch7* in the United Kingdom [26]. The result is a challenge to traditional sources of power, where trust is qualified rather than just given. Individuals are enabled to form trust decisions using their own data rather than information mediated by news sources. Of course, there are shortcomings to Mann's vision. For instance, there would need to be a change in the governance framework of a society so that individuals can access information that is currently closed, and also resourcing so that individuals can obtain the required technology. However, these limitations should not mean that the idea is dismissed. As Goldsmith [26] points out, the potential for individuals to perform some level of sousveillance increases with every improvement in camera technology.

Another example of practice that works genuinely in users' interests is the creation of digital environments that make users *aware* of the implications of their social network interactions. This alternative is a shift away from the majority of trust research that as far as possible claims that trust should be managed in the background and automatically handled by the digital system. The underlying objective is that trust in a digital environment should be a fluid state that it is not explicitly addressed by the user. This type of design can allow participants to attend to activities, whether that is shopping, finding a date or exploring a medical issue [27]. In contrast, we, the authors (as outlined in [27]), wish to create designs that make users mindful of their interactions so users become contributors to the wisdom of the digital ecosystems

they inhabit (in other words, the users are ‘strong links’). In particular, we wish to design a device that combines several factors (such as time, nearby devices and previous user preferences) in order to communicate an overall ‘comfort level’ to the user for the user to interpret. What the user does with this guidance is ultimately up to the user. The idea is to provide an opportunity for the user to have a ‘second thought’. Awareness can be created by ‘obstructive interfaces’, which could be as simple as a message to the user, “Are you sure that you really want to do this?’ Storey et al [28] have prepared a range of interface elements such as persistent, oversized, and insistent stop buttons and messages that require a deliberate hand action to dismiss. Different user’s require tailor made obstructions, add [29]. Nuanced communication styles for obstruction are a subject of further exploration. In previous research by the authors, [30] investigate Twitter messages coded as ‘trust’ by users as a means to understand how trust is conceptualised by users in social media networks.

Practitioners and researchers wishing to learn from users or to create systems that draw attention to the trust implications of interactions can learn from the research field of critical interactive design (see [31] for an overview), which is a subset of the larger practice known as Human computer interaction (HCI). Critical interactive design is working on similar notions of bringing in the user as an active participant and aims to create a space whereby a “user” can make a reflective choice about interaction. Within critical interaction design, there is the practice of 'seamful design' that aims to present to the user the ‘seams’ of a design; its constituent parts, and how it integrates with other systems [31]. The practice is a response to the automation culture we discussed earlier in this paper, the mission of mainstream technology designed to create interconnected, distributed systems that deliver ease and convenience seamlessly that are not noticed by the use. Within a seamful design, the biases, contradictions and problems of technology are exposed, rather than smoothed over by a design and a spirit of critique is engendered [31]. The role of researchers and designers is to identify which seams, out of all the possible data, will be important to the user and how best to present the seams.

As a final note, we add that as well as the trust community having something valuable to contribute to social network culture, social network data can be of use to trust researchers. Although social network data can be difficult to interrogate and reproduce scientifically (due to the control retained by the owners of social network sites), the data contains users discussing issues of importance to them within a ‘real world’ context. Trust researchers recognise how difficult it is to gather data from participants about trust either in laboratories, isolated from the impact of demands of everyday life or in the context of ‘real’ situations. In contrast, within social networks there are users around the world providing their view on trust in the form of publically accessible conversations in text format. Rather than a top-down view of trust, an abstract understanding developed by a researcher, social network data offers a ‘bottom-up’ view of trust from the perspectives of individuals. Sardana and Cohen [32] use social network data for this purpose and insert material from users to substantiate their trust models.

5 Conclusion

In conclusion, a critical approach to social media data use is necessary if social networks are not to become monopolised by commercial interests telling us who to trust and what trust means. A critical approach needs to: acknowledge and respond to the wider power relations that social networks generate and work genuinely in users' interests. Trust researchers can learn from the orientation of privacy researchers, to put the individual user first. Some trust researchers are already exploring from a user's perspective, investigating how to readdress information imbalances, to make users more attentive to the implications from interacting with social networks, and to enable users to form trust choices about their trust negotiations within social networks on their own terms.

References

1. Dalton C, Thatcher J (2014) What does a critical data studies look like, and why do we care? Seven points for a critical approach to "Big Data.". Society and Space Open Site
2. Garton L, Haythornthwaite C, Wellman B (2010) Studying online social networks.
3. Daly A (2015) The Law and Ethics of'Self Quantified'Health Information: An Australian Perspective. International Data Privacy Law (2015, Forthcoming)
4. Lupton D (2014) Beyond Techno-Utopia: Critical Approaches to Digital Health Technologies. Societies 4 (4):706-711
5. Walston SL, Bennett CJ, Al-Harbi A (2014) Understanding the factors affecting employees' perceived benefits of healthcare information technology. International Journal of Healthcare Management 7 (1):35-44
6. Fukuyama F (1995) Trust: The social virtues and the creation of prosperity. Free Press New York,
7. Kim Y, Ahmad MA (2013) Trust, distrust and lack of confidence of users in online social media-sharing communities. Knowledge-Based Systems 37:438-450
8. Sathi A (2014) Engaging Customers Using Big Data: How Marketing Analytics Are Transforming Business. Palgrave Macmillan,
9. Yu B, Chen M, Kwok L (2011) Toward predicting popularity of social marketing messages. In: Social Computing, Behavioral-Cultural Modeling and Prediction. Springer, pp 317-324
10. Johnson J From open data to information justice. In: Midwest Political Science Association Annual Conference, 2013.
11. Langlois G (2014) Meaning in the Age of Social Media. Palgrave Macmillan,
12. Ellison NB, Vitak J, Gray R, Lampe C (2014) Cultivating social resources on social network sites: Facebook relationship maintenance behaviors and their role in social capital processes. Journal of Computer-Mediated Communication
13. Liu G, Wang Y, Orgun MA Quality of trust for social trust path selection in complex social networks. In: Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: volume 1-Volume 1, 2010.

International Foundation for Autonomous Agents and Multiagent Systems, pp 1575-1576
14. Gupta R (2012) Has neoliberalism knocked feminism sideways? Centrestage,
15. Marx GT (2012) “Your Papers please”: personal and professional encounters with surveillance. Routledge Handbook of Surveillance Studies
16. Zelenko O, Felton E (2012) Framing perspectives on design and ethics. Design and Ethics: Reflections on Practice:3-9
17. Verbeek P-P (2011) Moralizing technology: Understanding and designing the morality of things. University of Chicago Press,
18. Stolterman E (2008) The nature of design practice and implications for interaction design research. International Journal of Design 2 (1):55-65
19. Pearson S, Tsiavos P (2014) Taking the Creative Commons beyond copyright: developing Smart Notices as user centric consent management systems for the cloud. International Journal of Cloud Computing 3 (1):94-124
20. Krontiris I, Langheinrich M, Shilton K (2014) Trust and privacy in mobile experience sharing: future challenges and avenues for research. Communications Magazine, IEEE 52 (8):50-55
21. Nurse JR, Pumphrey J, Gibson-Robinson T, Goldsmith M, Creese S Inferring social relationships from technology-level device connections. In: Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on, 2014. IEEE, pp 40-47
22. Netter M, Riesner M, Weber M, Pernul G Privacy Settings in Online Social Networks--Preferences, Perception, and Reality. In: System Sciences (HICSS), 2013 46th Hawaii International Conference on, 2013. IEEE, pp 3219-3228
23. Basu A, Vaidya J, Kikuchi H, Dimitrakos T Privacy-preserving collaborative filtering for the cloud. In: Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, 2011. IEEE, pp 223-230
24. Martinovic D, Ralevich V, McDougall J, Perklin M “You are what you play”: Breaching privacy and identifying users in online gaming. In: Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on, 2014. IEEE, pp 31-39
25. Mann S, Fung J, Lo R Cyborglogging with camera phones: Steps toward equiveillance. In: Proceedings of the 14th annual ACM international conference on Multimedia, 2006. ACM, pp 177-180
26. Goldsmith AJ (2010) Policing's new visibility. British Journal of Criminology:azq033
27. Marsh S, Wang Y, Noël S, Robart L, Stewart J Device Comfort for mobile health information accessibility. In: Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on, 2013. IEEE, pp 377-380
28. Storer T, Marsh S, Noël S, Esfandiari B, El-Khatib K, Briggs P, Renaud K, Bicakci MV Encouraging second thoughts: Obstructive user interfaces for raising security awareness. In: Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on, 2013. IEEE, pp 366-368
29. Murayama Y, Hikage N, Fujihara Y, Hauser C (2008) The structure of the sense of security, Anshin. In: Critical Information Infrastructures Security. Springer, pp 83-93

30. Dwyer N, Marsh S What can the hashtag# trust tell us about how users conceptualise trust? In: Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on, 2014. IEEE, pp 398-402
31. Boehner KA (2006) Interfaces with the ineffable. Cornell University,
32. Sardana N, Cohen R Validating trust models against realworld data sets. In: Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on, 2014. IEEE, pp 355-362