Managing Multiple Identities to Combat Stigmatisation in the Digital Age.

Tom Feltwell
Northumbria University
Newcastle upon Tyne, UK
tom.feltwell@northumbria.ac.uk

Shaun Lawson
Northumbria University
Newcastle upon Tyne, UK
shaun.lawson@northumbria.ac.uk

Ben Kirman
University of York
York, UK
ben.kirman@york.ac.uk

John Vines
Newcastle University
Newcastle upon Tyne, UK
john.vines@newcastle.ac.uk

Abstract
It has long been identified that people consciously curate, manage and maintain multiple online individual identities based on characteristics such as race, gender, and societal status; research has also established that people may choose to emphasise one such identity other another as a means to avoid stigmatisation, discrimination and stereotyping. The rise of online state, corporate, and peer surveillance however threatens to disrupt this process by modelling, categorising and restraining identity to that which has been surveilled. We posit that new anti-surveillance tactics may emerge that allow users the freedom to manage and switch their identities in ways that seek to maintain social justice and counteract discrimination.

Author Keywords
Stigmatisation; othering; digital identities;

ACM Classification Keywords
H.5.m. Information interfaces and presentation: Miscellaneous;

Introduction
Digital spaces allow for the expression of personal, societal and cultural identities, through diverse applications, websites and services. However, just as in offline spaces, fear and distrust of *the other*, a term to

denote those "not like us" [1], can manifest themselves, stigmatising and marginalising individuals. The power dimensions of online networks and social media and their influence on attitudes and behaviours at societal levels have been explored (e.g. [2]). Our own and others' perception of identity is multifaceted, composed of, amongst others, gender, race and cultural aspects, and often more "favourable" identities are accentuated in order to avoid stigmatisation [9]. This behaviour is extended to digital spaces, with the management, redefinition and separation of identities online being tailored to the platforms and audiences [3].

The ease with which digital surveillance is performed on our lives is increasingly ubiquitous given the integration of technology within our everyday lives, for instance through our use of smartphones, media platforms, social media and other web services. This was highlighted none more so than by the recent exposure of widespread state-sponsored surveillance by the NSA [7]. It is a logical step that such surveillance, as a by-product, can perform 'social sorting' [10] and therefore reinforce stereotypes that have the potential to stigmatise and, by extension, facilitate suspicion discrimination and even oppression. The current global threat of terrorism for instance has highlighted this issue (for a discussion of this in the UK see [12]).

Anti-Surveillance Tactics

Given this increasing intrusion and, propensity for oppression, it is natural to expect people to develop strategies to minimise and disrupt the online surveillance process in order render themselves free to express, and control, their identity. Evidence of these practices is well-established [4], with applications available perform random Google searches every 60 seconds using queries aggregated from news websites, in order to poison Google's surveillance by providing a generic, news-centric profile of the user [8]. Furthermore, the flexibility with which different digital mediums can be used affords users to tailor the medium to their requirements, aware of potential surveillance. boyd describes an analogous example where teens use private instant-messaging over Facebook communication in order to avoid parental surveillance [1]. Debating over the stigmatising effects of both anonymity and real name policies in digital platforms is already under discussion [5], with researchers highlighting the assumptions of singularity of identity to developers [6].

As surveillance becomes more prevalent, and datafication of our lives [11] more insidious, we speculate that these tactics will become more sophisticated and widespread, as a means to avoid being othered and stigmatised not only by peer groups but by the state and governments. By appropriating platform functionality to their own ends, modulating the mediums for communication and further technological responses to surveillance, users will continue to resist the defining nature of digital surveillance, in order to avoid becoming exposed to stigma and exclusion.

We see the HCI discipline as a fundamental part of this evolution in user behaviour. With HCI's increasing interest in politics and digital civics, we foresee that through adversarial design and similar approaches we as practitioners and researchers can accommodate, understand facilitate these requirements as part of socially just technology design.

References

1. danah boyd. 2014. It's Complicated: the social lives of networked teens. Yale University Press.
2. Manuel Castells. 2009. Communication power. Oxford University Press.
3. Stefanie Duguay. 2014. "He has a way gayer Facebook than I do": Investigating sexual identity disclosure on a social networking site. *new media & society.*
4. Benoit Dupont. 2008. Hacking the panipticon: Distributed online surveillance and resistance. *Sociology of Crime, Law and Deviance.*
5. Nicole Ellison. 2013. Future Identities: Changing identities in the UK – the next 10 years. *Foresight*.
6. Shelly D. Farnham and Elizabeth F. Churchill. 2011. Faceted identity, faceted lives: social and technical issues with being yourself online. In *Proc. of the ACM 2011 conference on Computer supported cooperative work* (CSCW '11).
7. Glenn Greenwald, Ewen MacAskill, and Laura Poitras. 2013. Edward Snowden: the whistleblower behind the NSA surveillance revelations. The Guardian 9.
8. Daniel C. Howe. 2015. TrackMeNot. Retrieved 14/01/15 from: https://addons.mozilla.org/en-US/firefox/addon/trackmenot/
9. Sonia K. Kang, and Galen V. Bodenhausen. 2015. Multiple identities in social perception and interaction: Challenges and opportunities. Annual review of psychology 66 547-574.
10. David Lyon. 2003. Surveillance as social sorting: Privacy, risk, and digital discrimination. *Psychology Press*.
11. Sue Newell and Marco Marabelli. 2015. Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'. *The Journal of Strategic Information Systems 24*, no. 1 3-14.
12. Tina Patel. 2011. Surveillance, suspicion and stigma within the 'war on terror' context.
13. Stephan Harold Riggins. 1997. The rhetoric of othering. The language and politics of exclusion: Others in discourse, 1-30.