What's in a name? Real name policies and social networks

Lilian Edwards
University of Strathclyde
Glasgow, UK
lilian.edwards@strathclyde.ac.uk

Derek McAuley
University of Nottingham
Nottingham, UK
derek.mcauley@nottingham.ac.uk

ABSTRACT
This paper surveys the controversial landscape of "real name" policies. While alleged to be desirable to promote social and polite behaviour online as well as accountability, such policies may have less obvious ulterior motivations, and may also have considerable undesirable consequences and threaten political freedom as well as freedom of speech. After an overview of legal solutions, we suggest the way forward may lie with a technical research programme that aims to replace the proprietary "walled garden" approach to social networks with a decentralised, dynamic and non-proprietary approach.

Categories and Subject Descriptors
Networks – *naming and addresing*; Security - *pseudonymity, anonymity and untraceability;* Human centered computing – *social networks.*

General Terms
Design, Security, Human Factors, Legal Aspects.

Keywords
Privacy, real names, anonymity, pseudonymity, Facebook, social networks, regulation

1. Introduction and global scene
Both the emerging disciplines of Web Science and Internet Science are conscious of the importance of social networking sites as increasingly the dominant mode of online communication, social participation and identity construction. In 2009, Nielsen Online reported that we now spent more time online on social networks than using email. In 2011, social networks such as Twitter were popularly credited (albeit with little supporting evidence) as the host and source of the outpouring of democratic movements known as the "Arab Spring". In 2012, Facebook hit one billion active users, with 2 billion predicted by 2014. In this context, requiring real names on social media networks has perhaps unsurprisingly, emerged as a controversial and significant policy. When Google+ was launched in 2011 with the more or less explicit selling point of not being Facebook, with its history of perceived anti-privacy attitudes (see [3,8] for context), supporters were dismayed [12] by the fledgling network's demand that real (or "common") names be used. Google's policy states:

"*Google+ makes connecting with people on the web more like connecting with people in the real world. Because of this, it's important to use your common name so that the people you want to connect with can find you. Your common name is the name your friends, family or coworkers usually call you. For example, if your legal name is Charles Jones Jr. but you normally use Chuck Jones or Junior Jones, any of these would be acceptable.*

If you are unable to complete the Google+ sign-up flow, or if your profile is or could be suspended for a name-related issue, review our guidelines below. If your profile name was already saved, and we find your name doesn't adhere to our Names Policy, you will have a four day grace period to change your name or appeal our finding before we take further action."[1]

Worse still, the search giant also followed this up by "nudging", if not compelling, users to link and prioritise real name use across various Google accounts held by a single user, even where registrations had already been validly obtained using pseudonyms, and where such "non-real" names were acceptable by prevalent norms (eg YouTube, Blogger[2]). Google's policy has received so much criticism that even Vint Cerf, one of the fathers of the Internet and now a senior Google employee was forced to comment on March 5 2013 that "Using real names is useful.. But I don't think it should be forced on people and I don't think we do." (Yahoo! News, Reuters, March 5 2013).

Facebook's real name policy[3] meanwhile has been attacked since inception and is known to be widely contravened by users[4]. In December 2012, the data protection regulator of Schleswig-

Web Sci 2013, Paris.

[1] See support answer "Google+ Page and Profile Names", http://support.google.com/plus/bin/answer.py?hl=en&answer=1228271

[2] See http://nakedsecurity.sophos.com/2012/07/26/google-pleads-for-youtube-real-name-use/ .

[3] See Facebook Terms of Service, as checked January 2013, at https://www.facebook.com/help/292517374180078/ .

[4] Facebook admitted 8.7% of its profiles or 83m profiles on Facebook were fake in their public accounts in August 2012.; http://www.guardian.co.uk/technology/2012/aug/02/facebook-83m-profiles-bogus-fake . The largest groups of "fake" profiles were pseudonymous duplicates (c 46m), "undesirable" profiles and profiles for user's pets.

Holstein in Germany issued a ruling that Facebook's real name policy contravened German Data protection law and must be dropped. The authority held that Facebook's policy of requiring its users to use their real names, with no provision permitting "pseudonymous accounts", violated the 2007 German Telemedia Act – specifically section 13, part 6 which states:

"*The service provider must enable the use of telemedia and payment for them to occur anonymously or via a pseudonym where this is technically possible and reasonable. The recipient of the service is to be informed about this possibility*.[5]"

German enforcement of privacy and data protection law is often much stricter than in other parts of the EU (notably "business–friendly" UK and, to a lesser extent, Ireland) but since the Data Protection Directive is EU-wide the decision is of pan European significance. Interestingly, although the Irish Data Protection Authority recently conducted an extensive privacy audit on Facebook[6] to see if it had adequately responded to a prior set of complaints raised in 2011, the matter of real name policies does not appear to be addressed, at least in the documents released to the public.

Mandating real names on communication networks as a matter of *governmental* rather than private or commercial policy has long been viewed in the democratic world as a policy of repression, associated with lack of political freedom and totalitarian surveillance. In China, where the state has a long history of exerting censorship control over the Internet, most ISPs and telecoms companies already routinely demand proof of real name for the service, so as to facilitate state surveillance, but China recently passed new laws mandating real name use on the Internet, which appear to extend beyond ISPs to popular microblog sites and possible even cybercafes[7]. And according to civil society blogger, academic and practicing lawyer, TJ McIntyre, even a Western democratic nation such as Ireland has recently considered a similar measure, partly prompted by the suicides of a well known politician said to have been the victims of cyber-bullying[8]. By contrast though, in South Korea, a democratic state emerging from a history of state control, the government has just abandoned a similar "real names" law, adopted in 2007 and dropped in 2011 after concerted public opposition and a Constitutional Court finding that such a law disproportionately restricted freedom of expression and did not achieve any public benefit[9].

2. Drivers towards, and negative consequences of, real name policies

The perceived advantages to governments of compulsory real names online are obvious in a world of post 9/11 security, ubiquitous surveillance and the perception of the Internet as a happy hunting ground for terrorists, paedophiles and organised crime. For private organisations such as Google and Facebook, the justifications follow a similar pattern: asserting the need to cut down on cyber-bullying, spam, online stalking, abuse and trolling.

The Electronic Frontier Foundation (EFF) summarise these motivations as follows: "that real names improve user behaviour and create a more civil environment; that real names help prevent against stalking and harassment by making it easier to go after offenders; that a policy requiring real names prevents law enforcement agents from "sneaking in" to the service to spy on users; that real names make users accountable for their actions [8]."

There are also arguments that real names are somehow "natural". Google claims on its Google+ real names policy page that in the real world people connect via their real ("common") names and this is something the online world should emulate, ignoring the long tradition of the Internet as a popular place for multiple roleplaying, often involving change of gender, age and nationality as well as mere name. Facebook combine the two agendas of control of abuse and trust in the online community in their statement: *"Facebook is a community where people use their real identities. We require everyone to provide their* ***real names****, so you always know who you're connecting with. This helps keep our community safe."*

A more cynical explanation for the apparent desire of private companies to aid public agendas of law and moral enforcement may lie in the commercial imperative to sell adverts – and increasingly, personalised, targeted or "behavioural" adverts as the main or sole revenue stream of these services. Online behavioural advertising or OBA depends on the accumulation of data about a user, which is turned by data mining techniques into a profile useful for commercial purpose (eg "24 year old male, based London, high income, owns BMW, likes science fiction movies and travel"). Such profiles are often processed as pseudonymous data and for most current commercial uses it seems pseudonymous profiles will do very well. However it seems not impossible to suspect that real names have become a *de facto* unique identifier in the social media space (where people do not readily reveal SSN numbers, passport numbers or credit card details as more conventional and useful unique IDs) making real name profiles even more potentially lucrative than pseudonymous ones. There can certainly be seen to be commercial incentives to acquire as complete a data profile as possible with a view to matching that data to other datasets for further data-mining. Acquisti et al [1] have shown that connecting someone's image to their Facebook profile is an easy route to access to their SSN number, and hence large amounts of useful information, by virtue of FB's real name policy. Large numbers of fake IDs are also seen as detrimental to a social network's profits by the markets, with

---

[5] See report at http://techcrunch.com/2012/12/18/facebook-users-must-be-allowed-to-use-pseudonyms-says-german-privacy-regulator-real-name-policy-erodes-online-freedoms/ . The decision was reversed in February 2013, not on the merits but on grounds that the Irish Data Protection authorities not the German DPA had jurisdiction: see http://techcrunch.com/2013/02/15/facebook-wins-court-challenge-in-germany-against-its-real-names-policy/ .

[6] Facebook Ireland Ltd: Report of Re-Audit, 21 September 2012, http://dataprotection.ie/docs/Facebook_Audit_Review_Report/1232.htm .The first audit report was published in December 2011 with provision for re audit in July 2012.

[7] See http://thenextweb.com/asia/2012/12/28/china-approves-regulations-that-introduce-real-name-registration-for-all-internet-users/ ; http://www.wired.com/threatlevel/2012/03/opinion_anxiaochinamicroblog /.

[8] See http://www.tjmcintyre.com/2013/01/legislation-is-not-answer-to-abuse-on.html .

[9] See http://www.chinadaily.com.cn/world/2011-08/11/content_13095102.htm .

the revelations of Facebook's fake ID population contributing to its slump in post IPO profits[10].

But the arguments against real names policies are manifold. Public regulators and private companies advocating real names policies, ostensibly to protect the vulnerable online, fail to note the many reasons why real names are as likely to imperil these users, eg by removing the protection of pseudonymity for political speech; exposing victims of domestic violence to stalking by ex-partners; LBGT people exploring their community online; and so forth[11]. *Wired* note that the real names imposed on China's thriving microblog scene are clearly intended to strengthen state lockdown on citizen speech online (see n 11) while the EFF [8] recall that offline anonymity to foster political speech has been upheld as a constitutional right in *McIntyre v. Ohio Elections Comm'n* 514 U.S. 334, 357 (1995) with the resounding assertion that:

"Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse."

At a personal level, many users find a real name policy is at best an annoyance, and at worst a potential bar on online participation. Stross argues [12] that real name policies are inherently broken as "there is no universal format for a human name". For children and young persons already suffering lockdown on their personal lives, Boyd and Marwick [3] observe that online is where they feel some safety and freedom – something a real names policy may jeopardise. Adults and children alike will feel constricted in their personal, sexual, work and community life by the assumption of a single or dominant identity and the inability to display different attributes in different social contexts [5 at part 2].

These problems are exacerbated by the massive increase in use of social networks as a form of "social surveillance" by employers and universities to vet potential hires and students [10, 11]. Bar an isolated case of German legislation, such scrutiny remains largely unrestricted by law, especially in the USA[12]. Harmful results also include the growing rash of cases of employee dismissal for blogging or other use of social media; and the growing trend of courts demanding social media passwords as part of litigation disclosure with associated privacy invasion. All of these abuses of privacy and restrictions on autonomy and diversity will be made easier if real name policies on private and public platforms become widespread and enforced.

At a practical level, real name policies worsen the consequences of security breaches without providing any guarantees of improving the social vices they are designed to combat. The Korean law was discredited after a hack attack disclosed the personal information of about 35m users of the country's popular Internet and social media sites Nate and Cyworld with user IDs, passwords, resident registration numbers, names, mobile phone numbers and email addresses all revealed (see n 13). The Korean Constitutional Court also concluded "there is no evidence that the real name system has significantly reduced the defamatory or otherwise wrongful posting of messages"

3. Legal solutions

Is there a legal right to pseudonymity online? The question, being relatively new, has never so far been raised in exactly this form in a European supreme court. In Europe, individuals have the right under article 8 of the European Convention on Human Rights (ECHR) to respect for their "private and family life", which has been interpreted in a very wide sense in some cases to include a right to "identity" (see Rodrigues 2011 [8] at 5.2.2.1.1) (eg right to change family name[13], right to end life, right to a national ID). The ECHR provides an enforceable remedy as individuals can take their case to the European Court of Human Rights even if their national law does not give them a remedy. But the ECHR does not as yet seem to offer a general right to pseudonymity, online or offline, and does not arguably go even as far as the US Supreme Court did in *Macintyre* in protecting *political* anonymity. Article 8 is weakened by being restricted by the need to also consider a number of public interest factors including "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". All of these provide ready excuses to exculpate the imposition of real names policies, and unlike in *Macintyre*, there is no presumptive preference given to free speech over public safety. Indeed, in the UK, one recent case has allowed the "unmasking" of a prominent pseudonymous political blogger and denied it was a breach of privacy on the grounds that "blogging is a public activity"[14]. An additional problem is that the doctrine of applying the ECHR to impose obligations on private bodies as opposed to the state – "horizontal effect" - is not yet clearly operable in many EU states.

At regional level, privacy is also regulated in the EC by the Data Protection Directive (DPD), which is currently in the process of protracted reform via the draft Data Protection Regulation (DPR) process[15] and is implemented with room for disparity in each EU member state[16]. Neither the DPD nor the DPR gives an unfettered right to anonymity or pseudonymity, and similar constraints apply to the guarantees of privacy it does give as in the article 8 case. So for example, the European Court of Justice in the case of *Promusicae*[17] refused to mandate that Spain had to pass laws

---

[10] See *Guardian* report at n 8 supra.

[11] See Geek Feminism Blog at http://geekfeminism.wikia.com /wiki/Who_is_harmed_by_a_"Real_Names"_policy? ; also n4 above and [7].

[12] The German legislation is discussed at "Germany Plans Limits on Facebook Use in Hiring", New York Times, Aug 25 2010. The new Californian law forbidding employers from demanding social media passports as a condition of employment is discussed at http://www.jdsupra.com/legalnews/new-california-social-media-privacy-law-47228/ .

[13] See *Burgharz v Switzerland* (1994) 18 EHRR 101.

[14] *The Author of a Blog v Times Newspaper* [2009] EWHC 1358 (QB), para 33.

[15] See http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf .

[16] For example in the UK by the Data Protection Act 1998.

[17] *Promusicae v Telefonica*, European Court of Justice, 29 January 2008.

requiring ISPs to disclose identities of subscribers to content industry rights holders who sought to identify alleged filesharers but needed ISP assistance to do so. Rather than declaring anonymity a right, all the case did was balance the competing interests of privacy and property rights and decide that Spain could not be compelled to pass such laws; but it was still open to other EU states to pass such disclosure laws (as indeed, most have).

For those who view real name policies as undesirable, then, current European law does not provide a ready remedy at the level of fundamental rights. Instrumentally, though, Data Protection (DP) law does, in theory, give users a chance to mitigate some of the potential harms caused by real name policies, by offering users tools (mainly, giving or withholding consent to processing) to restrain the collection, data mining and distribution of their personal data. In the case of social media, however, DP so far has largely failed to empower users, for the simple reason that most give away consent to processing of their personal data without thinking about it, as part of the sign up procedure for the network. Such consents are usually regarded as good enough for social networks, regardless of the fact that demonstrably most social network service users do not read their contract with the service provider (the "privacy policy"); do not understand it if they do; are unable to assess correctly future data-related risks; and cannot maintain vigilance over post-contractual changes in policies (Edwards 2013) [5].

The draft DPR recognises the problem of loss of control by users over data disclosure through online social network services as one of the key failures of DP law [EC Communication, 2010]. The DPR thus introduces several controversial new rights to enable users to more easily remove or delete their personal data, which they (or others) have released on social networks (and on other platforms). These rights include the hotly debated "right to forget" (article 17, DPR; Bernal, 2012 [2]) and to data portability. At time of writing however there are strong indications that, due to concerted lobbying from industry, especially the giants of the US such as Google and Facebook, combined with lukewarm concern for rights from nations such as the UK fearing economic consequences, these rights may either not make it to the final draft of the DPR or be so watered down as to make little difference[18].

Given the influence industry lobbying has had on the European, and indeed US, legislative process, which thus tends towards favour large data collecting industry rather than consumer and citizen rights, in enforcement if not in substantive law, it is likely better solutions for protecting users may come from "code" initiatives rather than privacy law: in the form of new types of distributed non-proprietary privacy-sensitive social networks where users cannot have real name policies imposed on them nor personal data collected and monetised against their will.

4. Code solutions

Many privacy-sensitive attempts so far at distributed social networking have focussed on "replace Facebook", aiming to replace the apparently dictatorial control of one network, with a new network which should be more responsive to the needs and rights of users. One of the leading contenders in this field is Diaspora, which was crowd-funded for development from 2010 on, although it has now become a "community" project run by volunteers with no remaining permanent staff. In September 2011, the developers stated, "...our distributed design means no big corporation will ever control Diaspora. Diaspora will never sell your social life to advertisers, and you won't have to conform to someone's arbitrary rules or look over your shoulder before you speak.[19]" These assertions were based on a design where the user's data was not served in the cloud under the control of the central network but retained on "pods" or servers, owned by the individual users. Similar ideas have also been expressed by Richard Stallman as part of his Freedom Box project.

Projects like Diaspora still have inherent, and crippling, limitations however. One is that it is almost impossible for them as new insurgents to combat the network effect of the incumbent, Facebook. They may not be under the control of a big corporation, but the downside of this is that your friends are unlikely to be there either. After three years (according to Wikipedia) Diaspora has around 375,000 accounts, in whatever state of activity, compared to Facebook's more than one billion active accounts. Rights of data portability, if ever finally conferred by the draft Data Protection regulation, may aid would-be Diasporans: but what are really needed are rights of data *inter*operability, enabling users to seamlessly interact with their friends on various social networks while retaining control over their own personal data and not subjecting themselves to the terms, conditions and real name policies of any single network, however large.

Accordingly, work is commencing within the RCUK funded CREATe Centre (Centre for Creativity, Regulation, Enterprise and Technology, see create.ac.uk) to build, not another social network, but tools intended to enable users to manage, ingather and control their data across a heterogeneous mix of platforms. Such tools would empower users to depart from proprietary and commercially operated services favouring a single "real" identity without fear of losing access to their friends and the services they want. Analogies can be drawn with 1980s networking technology: in that era a plethora of proprietary standards were fighting to achieve a dominate position, all of which became subsumed, not by the definition of yet another network, but by the definition of the concept of *internetworking* - an interface to permit applications to be implemented that were independent of the specific underlying networks. Likewise for social networks, the challenge is not how does yet another social network service replace all the others, but rather what is the "inter social networking" definition that permits social network independent applications to be constructed. AS well as technical challenges, the CREATe project will study the business model challenges – how can money be made from social interactions if not via the monetisation of personal data? – and sociological challenges – can community be constructed in networks formed dynamically by such internetworking tools? We hope to report back on these matters at the halfway point of the project in 2014.

5. ACKNOWLEDGMENTS

This work is supported by the RCUK through CREATe, the centre for copyright and new business models (AH/K000179/1).

[18] See note from Irish Presidency of the EU asking for more discussion on the right to be forgotten at http://edri.org/files/irl_dppaper.pdf .

[19] See http://blog.diasporafoundation.org/2011/09/21/diaspora-means-a-brighter-future-for-all-of-us.html , Sept 21 2011.

6. REFERENCES

1. Alessandro Acquisti, Ralph Gross, and Fred Stutzman, 2011 "Faces of Facebook: Privacy in the Age of Augmented Reality," *BlackHat USA*.
2. Bernal, P.A., 2011, 'A Right to Delete?', *European Journal of Law and Technology*, Vol. 2, No.2
3. Boyd, D. and E. Hargittai, 2010, 'Facebook privacy settings: who cares?', *First Monday 15(8),* http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589
4. Boyd, D. and A. Marwick, 2011, 'Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies', Draft paper for Privacy Law Scholars Conference, June 2011, Berkeley CA.
5. Brown, 2013 *Future Identities: Changing Identities in the UK – the next 10 years* , OII, University of Oxford, working paper for UK Foresight Project.
6. EC Communication, 2010, 'A Comprehensive Approach on Personal Data Protection in the European Union', Brussels, 4.11.2010 COM(2010) 609, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf .
7. Edwards L, 2013, "Anti-Social networking: social networks, privacy, law and code" in Brown I ed *Handbook of Internet Governance* (Edward Elgar)
8. EFF, 2011, "A Case for Pseudonyms", July 29, at https://www.eff.org/deeplinks/2011/07/case-pseudonyms
9. Rodrigues R, 2011, "Revisiting the Legal Regulation of Digital Identity in Light of Global Implementation and Local difference", *PhD thesis*, University of Edinburgh.
10. Sanchez-Abril P, 2012, "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee" American Business Law Journal, Vol. 49. Iss. 1
11. Saunders S.D., 2012, "Privacy is Dead: The Birth of Social Media Background Checks" 39 S.U. L. Rev. 243
12. Stross, 2012, "Why I'm Not on Google+", *Charlies Diary*, August 22, at http://www.antipope.org/charlie/blog-static/2011/08/why-im-not-on-google-plus.html