MANAGING ONLINE IDENTITY

Peter A P Clarke, Barrister at Law

INTRODUCTION

It is trite to suggest that most people assume and expect zones of privacy in their lives. Those zones, which vary from person to person and influenced by cultural and age factors, are not open for public inspection. Individuals decide when to give others personal information. Some information must be shared, such as by legislative requirement[1] while it is difficult not to provide some personal information to live comfortably and conduct business in a modern society[2]. In the non-digital world save for those who are public figures the default position is privacy and anonymity.

The reverse is true in cyberspace. The digital footprint one makes is not on cyber sand. It is often set in digital concrete. The accumulation of data makes the Internet a looking glass into at least part of the life of citizens. In the cyber sphere personal data is collected from a range of sources, the individual as well as the third parties. It is often openly available. Digital memories do not fade on line. They are fixed in text or image. Context is good fortune, not a given. This provides challenges in managing and maintaining an on line identity which is not distorted.

An invigorating aspect of the on line world has been the opportunity to engage in anonymous and pseudonymous speech. The development of algorithms designed to re identify data coupled with the aggregation of data threatens anonymity and pseudonomity on line and further exposes the individual to unwarranted scrutiny which has reputational consequences. Government initiatives and efforts by social media and business for users to have a universal identifier tied to their actual identity further has the prospect of reducing anonymous and pseudonymous speech and increases the ease within which a on line presence and interests can be accessed and analyzed.

---

[1] Income tax returns, social security,

[2] Opening a bank account, owing property,

The free flowing era of the Internet where the restrictions were free and usage limited is now a massive sprawling complex environment where data storage and retention is ubiquitous.

ANONYMOUS AND PSEUDONYMOUS COMMUNICATION

Anonymous and pseudonymous speech has a long history as a means of communication particularly in the United States. Between 1789 – 1809 six presidents, fifteen cabinet members, twenty senators and thirty four congressmen published anonymously or under *nome de plumes*.[3]

Anonymous communication allows for an individual to adopt diverse personas on line. Anonymous and pseudonymous communications have become ubiquitous on the Internet. The diversification of online social networks enables users to choose a community that suit their interests. In this way the Internet enables users to provide a "separate face" in a differing environment. Just as individuals have multi faceted appearances in their every day life, depending on the circumstances and the company this ability with the added benefit of anonymity is available on line.

The fragmentation and subdivision of interests and sites that cater from them coupled with the ability of visitors to contribute anonymously or pseudonomsly expands the contribution of those individuals to the public discourse. The protection offered by anonymity/pseudonymity allows for self expression without potential public ridicule or prurient interest. The practice is not universally positive as anonymity creates dangers of potential fraud, abuse, defamation and permits interference with other's privacy in the form of public disclosure of private facts and intrusion.

For the typical user on line anonymity or pseudonomity as to their web usage is illusory with respect to a determined effort to unmask the user. Through the use of cookies[4] and the fact that a user's Internet service provider ("ISP") has information that would link a screen name to one's actual identity web usage and the actual user is, in the main, traceable. The old joke may go "on the internet nobody knows you

---

[3] Daniel Solove, The future of reputation 140

[4] generally described as small text files downloaded into the user's computer when a user visits a web site

are a dog" but the more sober reality is that with time, effort and expertise and (hopefully) a legal basis someone sufficiently determined will know your breed, your favorite kibble and your favorite ball.

Through cross matching in cyberspace supposedly anonymised data can be re identified[5]. The capacity to de identify has expanded through the development of specifically designed algorithms to de anonymise previously anonymised networks[6]. One methodology being developed has focused on identifying users of two different anonymised social networks, Flickr and Instagram and Flickr and Twitter, with the aim of aggregating user profile information. The researchers cheerily admit they can make "..the bundled profiles available for end users as well as third party applications"[7] An anonymised dataset does not have to contain obvious identifiers for an individual to be identified and de anonymised. If an individual's patterns are unique enough outside information can be used to link the anonymised data to an individual[8]. There is no technical reason why algorithms cannot be developed to locate and re identify those who have opted for anonymity and pseudonimity and aggregate that data to obtain a detailed picture of one's on line identity in a short time intensive and more systematically than previously possible.

Fragmented identities are an irritant for business. From a commercial perspective business would prefer to tie an on line persona to a living breathing income earning and spending person. The most efficient and cost effective way of doing so is to have users convert their various online identities, named or pseudonymous, into one identifier which represents a verifiable human being.[9] A significant portion of the web economy is increasingly based on businesses accruing data that individuals provide as they search the net identifying what is read, what products have been

---

[5] In 2006 AOL Research posted 20,000,000 search queries of 650,000 users representing the usage over a 3 month activity. The information was purportedly anonymised. Nevertheless on line bloggers sorted through it and were able to identify users.

[6] De-anonymising social networks, Chen, Hu and Xie Stanford university December 10 2012

[7] ibid, introduction

[8] On a simple level a medical database was combined with voter lists to identify the health records of the governor of Massachusetts.[8]

[9] On the Internet, now everybody knows you're not a dog. ZdNet 20 February 2013

browsed and purchased. This data, collated, analyzed and refined, are sold for the purposes of marketing. It is now much easier tracking consumers wandering the web than following their journey through the high street[10].

Dominant social networks, such as Facebook[11] require users' on line identity to correspond to that of their offline persona. The development of such an identifier as a norm has the potential to establish a universal identifier within the cyber sphere, a development which dovetails in with the development of identify and access management technologies. A practical example is the use of Facebook identity to access music download sites such as Spotify and charity giving sites, such as JustGiving[12].

Business and public sector organisations are attracted to a means of authenticating users just once and provide them with access to resources, known as a single sign on ("SSO"). If linked with other sources of identity, Facebook, Google Paypal an SSO may act as a single point of access with "near failsafe means of establishing identity"[13]. The most advanced SSO systems may be standards based and designed for interoperability between organisations and linking them[14]. A concern for may occur where SSOs apply across other platforms where pseudonymous communication is currently respected. This protocol, and others such as OpenID, is touted as a hassle free and failsafe way of interacting on the Internet with no further need for multiple passwords and sign ins. Mozilla's open source browser based user authentication, Beta 2 of Persona[15] is a browser based decentralized authentication system that uses a verified email protocol applying public key cryptography to establish that a particular person owns their unique email address. It allows email providers to leverage their support for OpenID and another identity protocol, OAuth, used by Google and Yahoo.

---

[10] On the internet, now everybody knows you're not a dog, Steve Ranger, zdnet,com, 20 February 2013

[11] known as the Facebook Effect

[12] Digital identities and and the open business Quocirca February 2013 http://www.ca.com/ve/~/media/Files/IndustryResearch/quocirca-digital-identities.pdf

[13] Ibid 4

[14] Ibid 9

[15] previously known as BrowserID.

The corollary of this streamlining of access is potentially less flexibility in the future for those wishing to craft and manage their on line identity through pseudonymous activity. Universal identifiers arguably have a function when used to access governmental portals. Actual identity may be required for legislative compliance. In that regard the United Kingdom the Identity Assurance Program ("IAP") is being developed with PayPal, the Post Office. Experian, Verizon and others to create ways for the public to assert their identities in order to access government services. In the United States of America the National Strategy for Trusted Identities in Cyberspace ("NSTIC") has similar objectives. It, like its UK counterpart, focuses upon the cost of lack of security, identity theft and cyber crime with the current access and security arrangements on line. It mission is described in utopic terms:

> The *National Strategy for Trusted Identities in Cyberspace* describes a vision of the future—an Identity Ecosystem—where individuals, businesses, and other organizations enjoy greater trust and security as they conduct sensitive transactions online. The Identity Ecosystem is a user-centric online environment, a set of technologies, policies, and agreed upon standards that securely supports transactions ranging from anonymous to fully authenticated and from low to high value.
>
> Key attributes of the Identity Ecosystem include privacy, convenience, efficiency, ease-of-use, security, confidence, innovation, and choice. [16]

The claim (assertion) is that program such as the IAP and NSTIC shall give rise to more, not less, privacy on line [17] with the corresponding concession that anonymity will suffer.

REPUTATIONAL ISSUES

The purest treasure mortal times afford, is spotless reputation; that away, men are but gilded loam or painted clay[18].

Reputation has always been a valued asset within society. Its importance has been a regular theme in literature; Shakespeare's *Othello* to Miller's *The Crucible*, to name

---

[16] National Strategy for Trusted Identities in Cyberspace http://www.nist.gov/nstic/identity-ecosystem.html

[17] The Voucher business, the Economist 9 February 2013.

[18] Richard II, Act 1 sc 1 William Shakespeare.

but two prominent examples. Reputation has been defined by the Sociologist Steven Nock as "a shared, or collective, perception about a person." It has a particular context in societal as well as technical legal terms. Making amends or seeking to correct error which resulted in reputational damage was, and remains, an important task of those who value their reputations.

In common law jurisdictions the reputational impact of defamatory statements is clear as they are described as "tending to lower the reputation of plaintiff in the estimation of right thinking members of society generally"[19] , "are likely to injure the reputation of another, by exposing him to hatred, contempt or ridicule"[20] and/or the statements tend to make "..the plaintiff be shunned and avoided."[21]

Reputation is not only important for the individual it is a means by which that person will be initially judged and the basis upon which people will deal with him or her. In the past reputations were based almost exclusively upon the recommendation of trusted friends or acquaintances, community consensus, prior dealings, general notoriety and occasionally the media. Accordingly with such low tech means of delivery reputational growth was generally, but not always, relatively slow and the scope of one's reputation limited geographically.

An extraordinary feature of the Internet has been its impact on individuals or group's reputation, whether a rise or a fall. Scandal sheets of old have mutated into sites devoted to naming and shaming the relationship challenged[22]. The Internet expands and depersonalizes the way in which a reputation is built. It provides the raw material by which people can be judged but provides no nuance or weighting that in person communication invariably applies to such data. It is not the quiet conversation but a click of a switch that increasingly molds reputation in the current world. The permanence and the impact of prior mistakes do not fade with time. Whereas in the past memories would fade and remembrances would be changed by what Professor

[19] Sim v Stretch [1936] 2 All ER 1237,1240
[20] Parmiter v Coupland (1840) 6 M & W 105, 108
[21] Youssoupoff v Metro Goldwyn Mayer Pictures Ltd (1934) 50 TLR 581,587
[22] http://www.cheaterville.com/

Solove has described as "corrective of familiarity"[23] now whatever makes it onto cyberspace, whenever a comment was made or whenever images were taken, are as fresh and fixed in time as an insect found frozen in ancient amber. A teenager's twitter rant[24] or a photograph on Facebook depicting the consumption of an alcoholic beverage[25] is no longer an unpleasant but fading memory but a career limiting moment. This poses ongoing problems for users in managing their online identity.

Traditionally the means of correcting error to a publication was by way of responding article or obtaining from the publisher a correction or, even better, an apology. There was no guarantee of having a responding article printed or read and corrections and apologies are less common that an aggrieved party would hope. Cyberspace permits a quick countervailing response to a slur. That said there is scope for expanded reputational damage associated with internet shaming, complaints going viral and slurs being published broadly and beyond the bricks and mortar in which the individual resides.

The great informal protection mechanism that has, until recently, aided privacy is the practical difficulty of intruding into another's life on a continuous basis. Tracking individuals' movements has been historically difficult and costly. Governments of whatever shade have sought to maintain some form of knowledge of its subjects, if for no other reason than to maximize tax revenue[26]. The inefficiency and cost of tracking one let alone many individuals, not to mention the need for maintaining records of those endeavors have complicated any effective means to de anonymise the activities of on line users. Aggregation of data and algorithms has changed this dynamic.

LEGAL PROTECTIONS

In the US legal system there is a strong and entrenched constitutional protection of anonymous political speech. The right to anonymous association and anonymous communication are seen to play an important, if not intrinsic role in political discourse. That said the First Amendment limits one traditional legal method of

---

[23] The Future of reputation

[24] UK youth Commissioner under fire over foul tweets
http://www.abc.net.au/worldtoday/content/2013/s3731935.htm

[25] I know who you are and I saw what you did Lori Andrews 122-123

[26] arguably the underpinning rationale of William the First of England's Doomsday Book

defending reputation on line, the defamation suit. American defamation law has developed to conform to the First Amendment. This has reduced its potential efficacy as a cause of action when compared to other common law jurisdictions.

The tort of public disclosure of private facts is the most likely tort for enforcement of privacy rights on line. It deals with unwanted dissemination of personal rights. In this respect also American courts have consistently found that rights of freedom of speech trump the privacy rights when involving the press. When tort injury conflicts with free speech the latter will invariably win. The Supreme Court in *Cox Broadcasting v Cohn*[27], *Smith v Daily Mail Publishing*[28] and *Florida Star v B.J.F*[29] have circumscribed the operation of the tort. In *Cox* the Court found for a television station which identified a deceased rape victim stating " the interests in privacy fade when the information involved already appears on the public record."[30] In *Smith* the Court found there is no liability for publishing information lawfully acquired and in the public interest unless the state interest of is of the highest order. In *Florida Star* the Court found that the publisher of truthful information, lawfully obtained is only liable only when contrary to a state interest of the highest order. As a consequence the tort is seen to be ineffective in protecting privacy rights, particularly involving the media. Regarding reputation the Supreme Court was even more emphatic in *Butterworth v Smith*[31] stating "Absent exceptional circumstances, reputational interests alone cannot justify the proscription of truthful speech.[32]

The approach taken in Australia, New Zealand and the United Kingdom provide a means by which material which is defamatory, and other material which may give rise to a criminal or civil action, may be removed. In Australia section 91 of the *Broadcasting Services* Act 1992 provides Internet content hosts and ISPs with a measure of protection from liability for material which may attract suit under statute or in common law or equity with respect to material posted on line by their subscribers. The effectiveness of the section for the offended party is in once an

---

[27] 420 US 469, 493 - 96
[28] 443 U.S. 97, 105-6
[29] 491 U.S. 524
[30] at 494 -495
[31] 494 U.S. 624
[32] at 634

internet content host or internet service provider knows that it is hosting, caching or carrying offending material the section 91 defence ceases to provide them with a defence relating to the cause of action contemplated. If the material continues to be accessible, then the host or provider is potentially liable under the usual elements of the action brought by an aggrieved party. Regulations 18 and 19 of the *Electronic Commerce* Regulation protect service provides from liability in the United Kingdom for caching or hosting material provided that upon obtaining actual knowledge or awareness of the material the providers act expeditiously to remove or disable access to it. There is, as such, effective incentive for ISPs to remove egregious material.

Neither Australia or the United Kingdom have a tort of privacy. Privacy actions are grounded in equity as a breach of confidence action. Equity has recognized a right to personal property under the rubric of breach of confidence since the nineteenth century. In *Abernethy v Hutchinson*[33] (*Abernethy*) the Lord Chancellor determined that private documents would attract protection in equity. The protection was framed in the form of trust rather than the previously based protections grounded in property[34] In *Prince Albert v Strange*[35], like *Abernethy*, the protection was not of valuable secrets exploited in traditional occupations. It involved the individual's concern to retain a sphere of personal control of information of a private and professional character. *Abernethy* and *Prince Albert* laid the groundwork of a doctrine regarding the surreptitious or improper obtaining of private or personal information including where there is no pre existing relationship of confidence. In *Francome v Mirror Group Newspapers Ltd*[36] the United Kingdom Court of Appeal accepted that publication of surreptitiously obtained information would be a breach of confidence. In *Giller v Procopets*[37] an Australian decision found that damages were available for breach of confidence for misuse of private information and that distress was a sufficient damage to give rise to actionable claim.

---

[33] (1825) 1 H & Tw28; 47 ER 1313
[34] see *Pope v Curl* (1741) 2 Atk 342, *Millar v Taylor* (1786) 4 Burr 2303, *Donaldson v Beckett* (1744) 4 Burr 2408 and *Gee v Pritchard* (1818) 2 Swans 402).
[35] (1849) 1 H & Tw 1
[36] [1984] 2 All ER 408
[37] the Victorian Court of Appeal, *per* Ashley and Neave JA,

In the United Kingdom the House of Lords decision in *Campbell v Mirror Group Newspapers*[38] awarded damages for breach of confidence involving the misuse of private information. A key element in a breach of confidence action, that the information was imparted in circumstances giving rise to an obligation of confidence[39] does not fit comfortably in privacy actions. Many instances of privacy violation occur where there is no pre- existing relationship of confidence, such as the relationship between and individual and media organizations. That is particularly so in cyber sphere. Breach of confidence is not, under its current construction, suited to all situations where one person invades the privacy of another, particularly when the parties involved are strangers and do not hold obligations of confidence to one another. Not all privacy actions are information-related. Breach of confidence actions permit the injunctive relief as a form of relief. This is relevant when considering removing material from the Internet.

European laws are intended to safeguard an individual's dignity and public image. The European Convention on Human Rights requires a balance between the Article 10, the right to freedom of expression, and Article 8, a right to privacy. It has become part of the laws of the United Kingdom.[40] The European Union has proposed recognition of the recognition of a right to be forgotten that would allow individuals to demand permanent removal of their personal data. The Privacy Directive states that the laws of member states must ensure personal information is kept in a form which permits identification of data subtext for no longer than is necessary for the purposes for which the data were collected and that each person ahs the right to obtained erase or blacking of data which has been kept for longer than necessary.[41] The right would not apply where it would conflict with the freedom of expression of journalists or with freedom of artistic or literary expression. It is a further exception where individuals engage in purely personal or household activities.

[38] [2004] 2 AC 457
[39] *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41
[40] by virtue of the Human Rights Act 1998
[41] Article 12

PRACTICAL MEANS OF MAINTAINING ON LINE IDENTITY

There is a burgeoning market for those who wish to tidy up their reputations[42], many advertising on Google whose retention policy gives them the greatest source of business and their clients the greatest angst. The Reputation communities effect is limited. Generally they can attempt to get problematic information or photographs from the web. Regarding items that a user wants removed the service typically writes to the website operator requesting its removal. But as the founder of Reputation.com has said "there is no silver bullet… If there was I'd be a billionaire already."[43]

One means of browsing without creating a digital trail is to cleaning out a cache of cookies on the computer. While this is easily done through accessing the preferences option and clicking the delete cookies option the right of auto log in and personal customization and personalization of sites traditionally visited will be deleted. A more thorough method of clearing up cookies is available through downloading specific programs to clean up Internet history, cookies, auto complete forms, index files and flash cookies.[44] A less technical approach is to delete accounts to websites no longer frequented. Programs exist which purportedly keeping Facebook in check while programs[45] which disable third party tracking, depersonalize searches, identify and block information requests from websites are also possible options.

Using Google alerts to send email updates every time a persons name is queried assists in monitoring the information other people are looking regarding a user and where they are accessing it from. Using the program Googlesharing allows users to search through Google without being tracked. The technology scrambles the search requests through Google without being tracked.

In terms of personal maintenance the options include purchasing one's own domain name. Through a number of programs and sites[46], it is possible to place content within these sites and optimizing presence on social sites.

---

[42] www.reputationchanger.com, www.onlinereputationcorrection.com, manageyourinternetreputation.com, www.reputation.com,
[43] Reputation.com frequently asked questions.
[44] CCleaner and Flash Cookie Cleaner
[45] such as Disconnect or Facebook Disconnect for Chrome browser users.
[46] such as Tumble, Wordpress and Aboutme

Notwithstanding all of the above, even with the use of services or one's own sweat and tears removal of photos or shutting down of pages the content may and probably will be found on the Internet. Archiving by private organisations may thwart the best efforts. The Waybackmachine, a project which takes screenshots of websites across time and archives them to preserve a copy of the Internet, precludes substantial control of material relating to one's own identity.

Circumvention proxy anonymity software is a solution for those who are technically savvy and such as Tor and Freegate permit some form of anonymity as does remailing services.

CONCLUSION

The management of on line identity and associated reputation is becoming more complicated. The ability to trace ISP addresses always poses a threat to anonymous and pseudonymous speech. The use of algorithms and the aggregation of data and the reidentification militates against users having a multi faceted life on the web.

The protections afforded by the tort of privacy and defamation in the American context are of only limited effect in affording appropriate protections. The options are greater in other common law jurisdictions but still limited.

For those determined enough scrubbing data through their own efforts or those of a service has some utility but only to the extent that the suasion will allow. Other options such as positive placement or rejigging Google placements to minimize exposure has some utility but are far from complete solutions to a growing challenge.

REFERENCES

The Court of Public Opinion Is About Mob Justice and Reputation as Revenge, Wired 26 March 2013 http://www.wired.com/opinion/2013/02/court-of-public-opinion/

Truth, Lies, and 'Doxxing': The Real Moral of the Gawker/Reddit Story Wired 29 October 2012 http://www.wired.com/opinion/2012/10/truth-lies-doxxing-internet-vigilanteism/

You are what Google Says you are Wired, 11 February 2009 http://www.wired.com/business/2009/02/you-are-what-go/

The Law of Defamation and the Internet (3rd Edition) Matthew Collins Oxford

Electronic Theft Unlawful Acquisition in cyberspace Cambridge

The Transparent Society David Brin Perseus Books

The voucher Business, the Economist 9 February 2013

The identity perimeter September 2012, Quorcirca and Ping Identity

The Right to erasure protects people's to forget the past says expert, The Guardian, 4 April 2013

Susan Adams, 6 Steps to managing your Online Reputation 14 March 2013

Kashmir Hill, *One Line Reputation Managers want to help remove your digital tattoos* Forbes, 6 April 2011

Corbett, *Qualifying the value of anonymous and pseudonymous communications in an online Social Network*. Chapel Hill. North Carolina April 2010

Bilton, *Erasing the Digital Past* New York Times 1 April 2011

Sanur Sharma, Preeti Gupta and Vishal Bhatnagar, *Anonymisation in social network: a literature survey and classification*, In. J. Social Network Mining Vol 1 No 1 2012, 51

Prateek Mittal, Charalampos Papamanthou, Dawn Song, *Preserving Link Privacy in Social Network Based Systems* University of California Berkley

A. Michael Froomkin, *Anonymity and the Law in the United States*, 2008

Yves-Alexandre de Montjoye, Cesar A Hidalgo, Michael Verleysen & Vincent D Blondel, Unique in the Crowd: The privacy bounds of human mobility, Nature.com

A Michael Froomkin, *Lessons Learned Too Well*, Miami Law Research Paper Series 22 September 2011

Oana Goga, Howard Lei, Sree Hari Krishnan Parthasarathi, Gerald Friedland, Robin Sommer and Renata Teixeira On Exploiting Innocuous User Activity for Correlating Accounts Across Social Network Sites May 2012

Arvind Narayanan and Vitaly Shmatikov *De – anonymizing Social Networks*, University of Texis at Austin

The Price of Reputation, The Economist 23 February 2013

Steve Ranger, On the internet, now everybody knows your not a dog, Zdnet,com, 20 February 2013

Steve Ranger, The data black hole that could suck the life out of the internet economy Zdnet,com 8 February 2013

Danqi Chen, Botai Hu, Shuo Xie *De-anonymizing Social Networks* Stanford University 10 December 2012

Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of anonymisation* 57 UCLA Law Review 1701 (2010)

Ken D Kumayana *A right to pseudonymity* Arizona Law Review [Vol 51:427]

Daniel J Solove *The Future of Reputation* Yale University Press 2007

Daniel Solove, *Marc Rotenberg and Paul M Schwarz, Privacy, Information and Technology* Aspen Publishers 2006

Lori Andrews *I know who you are and I saw what you* did Free Press 2011

Lawrence Lessig, *Code Version 2.0* Basic Books 2006

Daniel Solove *Nothing to Hide* Yale University Press 2011

Jeffrey Rosen *The unwanted Gaze* Vintage Books 2001

Daniel Solove *The Digital Person* New York University Press 2004