scripted

Volume 12, Issue 1, June 2015

YOU CAN'T ALWAYS GET WHAT YOU WANT[1]: RELATIVE ANONYMITY IN CYBERSPACE

Sara Nogueira Silva**[*] and Chris Reed[†]

Abstract

Cyberspace is changing the way we communicate, live and interact. Most significantly, it changes the nature of anonymous communication. In the physical world we all have a reasonable understanding of how anonymity can be achieved, but cyberspace was not designed to work the same way as real space. Machine communications contain information which identifies their originating machine, and internet service providers (ISPs), internet businesses and online social networks (OSN) can often identify users via the information that users disclose to them. As such, once users communicate online for the first time their anonymity starts to become compromised.

Most discussions about anonymity assume that anonymity has some binary, on/off value. They ignore that the way we communicate has been changed by cyberspace; and also overlook the fact that even individual users are often able to identify someone by simply collecting and connecting the information available online. This means that users who freely decided to make information available online in a particular situation, where that information is available to the masses, cannot expect not to be named in another different situation.

In the digital age, users are living in an anonymity limbo[2] where they may not yet be named but can potentially become so at any time. As such, it seems inevitable that this new reality around anonymity will have implications on the two concepts often linked to it: autonomy and consent.

---

[1] The Rolling Stones song´s title.

[*] PhD candidate, School of Law, Queen Mary University of London.

[†] Professor of Electronic Commerce Law, School of Law, Queen Mary University of London.

[2] See Figure 1.

DOI: 10.2966/scrip.120115.35

1. The traditional concept of anonymity

Dictionaries define anonymity as the state of remaining unknown to most other people, or a condition of being anonymous.[3] Anonymous comes from the Latin expression, which means 'nameless', [4] without a name.[5] Someone anonymous is a person who is unnamed, unidentified, unknown, unspecified, undesignated, unseen[6] or unacknowledged.[7] Anonymity is not a simple question whether I am or not identified, but rather, whether I do or do not feel known.[8] According to Burkell "anonymity is not an all or nothing condition"[9] but a complex operational concept.

Social sciences have been defining anonymity: as an element of the concept of deindividuation[10] or interpersonal disconnectedness, [11] which entails that there exists an inability of others to identify the individual;[12] and as an element of the concept of impersonality, detached from any possibility to be identified or attached to an individual.[13] This "anonymity in the city" reflects social distance and lack of distinction among others.[14] Furthermore, anonymity involves one's individual ability to exert boundary control upon others' access to one's self,[15] and that anonymity allows a sense of self-government and a greater range of self-expression.[16] Anonymity reduces social anxiety and the risk of retaliation. [17] The legal approach to anonymity, traditionally, is much more simplistic; a person is anonymous if that person is not, at present, identified.

Of course, even in the real world it is sometimes possible to overturn a person's anonymity through detailed investigation. In late 2013 the Van Gogh Museum

---

[3] Definition found at Oxford Dictionaries available at http://www.oxforddictionaries.com/definition/english/anonymity?q=anonymity (accessed 1 Dec 2014).

[4] Ibid.

[5] J Burkell "Anonymity in Behavioural Research: Not Being Unnamed, But Being Unknown" (2006) 3 *University of Ottawa Law & Technology Journal* 189-203, at 192.

[6] Ibid, at 197

[7] See note 3 above.

[8] See note 5 above, at 202.

[9] See note 5 above, at 203.

[10] P Zimbardo, "The human choice: Individuation, reason and order, versus deindividuation, impulse and chaos" (1969) *Nebraska Symposium on Motivation*, University of Nebraska Press; C Haney, W Banks and P Zimbardo, "Interpersonal dynamics in a simulated prison"(1973) 1 *International Journal of Criminology and Penology* 69–97; A Zimmerman, "Online Aggression : The Influences of Anonymity and Social Modelling" (2012) University of North Florida available at http://digitalcommons.unf.edu/etd/403/ (accessed 1 Dec 2014).

[11] See note 5 above, at 193.

[12] A Zimmerman, "Online Aggression : The Influences of Anonymity and Social Modelling" (2012) University of North Florida available at http://digitalcommons.unf.edu/etd/403/ (accessed 1 Dec 2014).

[13] Ibid.

[14] See note 11 above.

[15] D Pedersen, "Psychological functions of privacy" (1997) 17 *Journal of Environmental Psychology* 147-156, at 149

[16] See note 12 above, at 4.

[17] See note 5 above.

confirmed[18] that the *Sunset at Montmajour* was painted by the Dutch artist Vincent van Gogh in July 1888.[19] In the 1990´s, the museum had refused to attribute the painting to Van Gogh partly because it was anonymous. However, after exhaustive examination of the painting and analysis of documents related to the artist,[20] researchers were able to match the painting with the painter´s techniques and materials. More relevant, they uncovered a letter where the painter described to his brother the landscape that he was painting on the day before, which was the precise description of the *Sunset at Montmajour*.[21] The researchers were trying to match the information they had about the anonymous painting with the information that they kept about the identified painter Van Gogh, in order to identify the authorship.

This is a good example to explain how robust anonymity is in the real world. In this case, the painter was anonymous until the researchers, after long and painstaking investigation, concluded that Van Gogh was the person who painted the *Sunset at Montmajour***.** This tells us that in the real world, anonymity as it has been defined, as a state of remaining unknown to most other people, or a condition of being unnamed, unidentified, unknown, unspecified, undesignated, unacknowledged, does not exist as an absolute concept. If sufficient information is discoverable, an anonymous person can be identified. In our example, the painter was only anonymous until someone decided to research who he was and found the information connecting the painting to Van Gogh.

But the time, effort and facilities needed to conduct such an investigation are substantial. It is clear that the Van Gogh Museum has resources to conduct such research that are beyond the common citizen. This limitation on the process of identification in the real world means that, for most practical purposes, anonymity can be treated as a binary state, either subsisting or not subsisting. However, in the online world technology is breaking such limitations, and even the common citizen has access to a huge amount of information resources. As a result, the relative strength of anonymity is far weaker in the online world.

Anonymity has real social importance, particularly in maintaining personal autonomy and facilitating free speech. A significant consequence of the rise of online technologies is that the anonymity question has changed. It is no longer enough for the law to ask whether a person should be identified, or even whether a particular piece of potentially identifying information should be disclosed. Instead, the proper question is whether information should be collected at all, even if each individual item of information is apparently no risk to anonymity.

2. Anonymity in Cyberspace – a relative concept

From the mid- 1990s the internet came into our world creating a new vision of social, political and personal freedom. In cyberspace,[22] a person could express their social and political views to an unprecedented worldwide audience without any fear of being

[18] Reported at Van Gogh Museum website available at http://www.vangoghmuseum.nl/vgm/index.jsp?page=330726&lang=en (accessed 1 Dec 2014).

[19] Reported at BBC News website available at http://www.bbc.co.uk/news/entertainment-arts-24014186 (accessed 1 Dec 2014).

[20] See note 18 above.

[21] See note 19 above.

[22] For the purpose of this research, real world is defined as the physical and off-line environment, while cyberspace and online world is defined as computer-based environment.

identified; and a person could be whoever they chose to be without fear of preconception and discrimination.[23] Cyberspace was a representation of freedom and autonomy reinforced by anonymity. This is what psychologists describe as Cyberdisinhibition.[24] In 1999 Lessig wrote:

> Relative anonymity, decentralized distribution, multiple points of access, no necessary tie to geography, no simple system to identify content, tools of encryption – all these features and consequences of the internet protocol make it difficult to control speech in cyberspace.[25]

However, the experience of being anonymous turned out to be a myth.[26] All of a user's activities in cyberspace can be linked with a machine, unless unusual precautions are taken,[27] and can thus potentially be identified. Even in 1999 Lessig could see what was likely to happen.[28] Because of the development of cyberspace, and in particular the ease and cheapness of collecting any and all data which passes through an internet server, the online world raises additional challenges to the anonymity concept.[29]

Nowadays, ISPs and other Internet companies such as Google and Facebook, using advanced resources, have access to an enormous amount of information. With specific tools, those Internet companies can easily name a previously anonymous person and determine his/her profile. In addition, with less sophistication, any citizen who uses the internet has also unprecedented access to the resources and information to uncover someone´s identity through what we call "my search and research". We create this term to define the process of a normal user's online search, whereby they are able to identify someone by the process of search and research online; by connecting and collecting

---

[23] J Barlow, "A Declaration of the Independence of Cyberspace" (Feb. 9, 1996) *Electronic Frontier Foundation* available at http://www.eff.org/barlow (accessed 1 Dec 2014).

[24] Cyberdisinhibition was a term coined by Daniel Goleman, as referred in, P Eastwick and L Gardner, "Is it a Game? Evidence for Social Influence in the Virtual World" (2009) 4 *Social Influence* 18-32, at 6.

[25] L Lessig, *Code and other laws of cyberspace* (New York: Basic Books 1999) 236.

[26] D Solove, "The PII problem: Privacy and a New Concept of Personally Identifiable Information" (2011) *New York University Law Review* 1814–1894.

[27] Eg. The use of anonymising proxies or other anonymising services. Even so, the user will still be potentially identifiable by the operator of the anonymising service, and so the strength of his or her relative anonymity depends on whether the service provider will, or can in the face of law enforcement, keep that identifying information secret.

[28] L Lessig, "The Law of the Horse: What Cyberlaw Might Teach", (1999) 113 *Harvard Law Review* 501, 510:

> The architecture of cyberspace does not similarly flush out the spy. We wander through cyberspace, unaware of the technologies that gather and track our behaviour. We cannot function in life if we assume that everywhere we go such information is collected. Collection practices differ, depending on the site and its objectives. To consent to being tracked, we must know that data is being collected. But the architecture disables (relative to real space) our ability to know when we are being monitored, and to take steps to limit that monitoring.

[29] This is partly because of technological change, which enables information to be collected about a user's prior and subsequent activities in addition to the mere content of that user's communication. "Cyberspace has no nature; it has no particular architecture which cannot be changed." Lessig, ibid 505. But even more important is the change in the architecture of the business models of the enterprises which make up the internet, who fund their activities by collecting and recording all the data they can and bringing that data together in searchable form.

information, as we will demonstrate. As we shall see, these possibilities make it impossible to assert an absolute right to anonymity online.

To understand how anonymity is shifting nowadays we should examine the technology that facilitates internet users to go online by attributing to them an Internet Protocol (IP) address. A citizen who desires to have access to the online world will need a computer, laptop, tablet or a smartphone as a first requirement. Then, in order to get such access, the user will have to arrange with an Internet Service Provider (ISP) in the country of residence to provide Internet access. The ISP will require personal details in order to provide the service. Once terms and conditions of the contract are agreed, the ISP will permit internet access via attributing an IP address to the account holder's connecting machine.[30] Using this internet connection, the citizen will be able to setup or check his/her email accounts and have access to the unprecedented amount of information that the web offers.

The user's communications are not absolutely anonymous because the ISP knows the account holder details and can link them to the IP address from which each communication originated. The ISP records the IP address every time a user accesses the online world and can thus also identify which sites he/she visited because each site has its own IP address. The IP address record held by the ISPs is a fingerprint containing an enormous amount of information about the account holder's online navigation pattern.[31]

This example brings interesting features to anonymity. When users access the internet through a machine, there is immediately a potential possibility to identify them. This is because machine and electronic communications can be linked with a user, i.e. they are not absolutely anonymous. This tells us that anonymity needs to be understood as a *relative* concept, not as an absolute one.[32] As soon as he/she accesses the internet the user is no longer unidentifiable because some information is known about him/her. This may not allow us to name the individual yet, but it can provide enough knowledge about that nameless person so that he/she can be *singularized* from others and linked to specific online actions. The person is now singularized within the masses but is still a nameless person, and so continues to enjoy some degree of anonymity. However, that anonymity state is fragile. In fact, some extra collection and connection of information will potentially lead to the disclosure of the user's name. Thus, anonymity seems to stand as a relative and ephemeral state that flows through this range from unidentifiable to singularized and finally becoming named, and that state changes from time to time. Once you are named you stop being anonymous. Users in cyberspace are living in a relative

---

[30] *Data Retention Regulations 2009/859*, Sch 1 Communications data to be retained, part 3 internet access, internet E-mail or internet telephony, para. 13 (1) (b) presents two types of IP address dynamic or static. The dynamic IP address is the most common type that ISP provides to users because it is more cost-benefit. A dynamic IP address is allocated to a specific user from a pool of IP addresses changing from time to time; while a static IP address remains unchanged.

[31] Usually a dynamic address, linked to the account via ISP records. This IP address relates to all uses of the account, and thus may include all the people who live at the same address and have access via the account.

[32] Social sciences have been analysing the influence of anonymity in social behaviour and they supported that anonymity is not a monolithic concept, but a complex and varied concept, which can influence numerous behaviours, see further, J Burkell "Anonymity in Behavioural Research: Not Being Unnamed, But Being Unknown" (2006) 3 *University of Ottawa Law & Technology Journal* 189-203, at 193.

anonymity limbo where they are not yet named, and perhaps not even singularized, but they can easily become so.

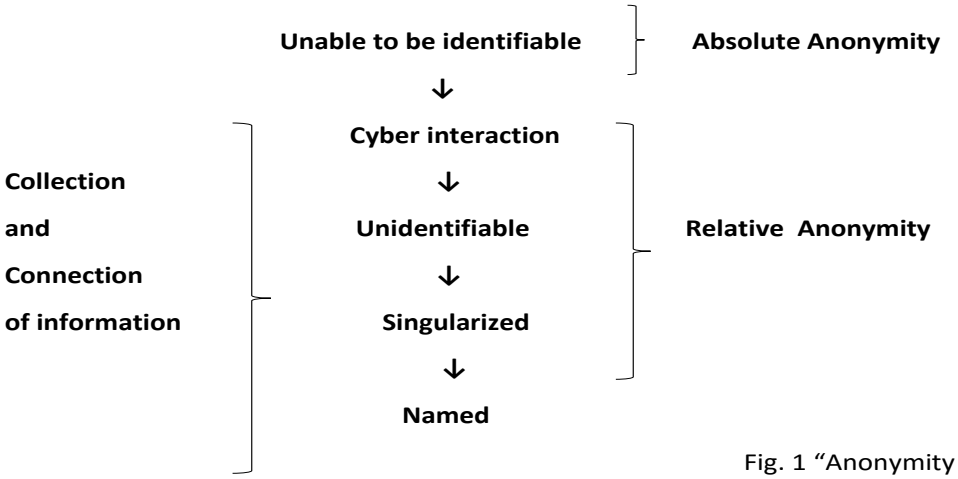

Fig. 1 "Anonymity limbo"

This perspective is wider than that of Daniel Solove when he describes traceable anonymity.[33] He argues, "whenever one is online, a potential for traceability exists".[34] Accordingly, traceability involves the extent to which anonymous posts can be traced to the author´s true identity.[35] From the analysis of how an ISP can identify users, an argument for traceability seems coherent. However, Solove's main concern is with tracing users' activities via their IP addresses, an activity which is restricted to ISPs and those who can gain access to their records, eg via court orders. Solove did not take into consideration two other factors which impact anonymity: the role of internet businesses, such as search engines and OSN, who generate and store information about users; and the searches that normal users can undertake using less sophisticated data matching ("my search and research" as we will explain),[36] which potentially lead to identification.

Internet businesses have been using technology to access users' details in ways which singularize them but do not name them. However, the quantity and detail of the information collected is such that a nameless person might be easily named by means of further collection or connection of information (fig.1.). Search engines, online shopping sites, "chat rooms", OSN and blogs are the most relevant agents of the internet business. Such companies have developed new business platforms based on the value of the information about each user's online activities and communications.

Users rely on search engines such as Google to find information online. When a user types a search term, those sites will keep details of what the users searched for, which key

[33] D Solove, *The Future of Reputation: Gossip, Rumour, and Privacy on the Internet* (Yale University Press, 2007).

[34] Ibid, 146.

[35] See note 33 above.

[36] In fact, with less sophistication any user has also unprecedented access to an infinite amount of resources and information to uncover someone's identity, by collecting and connecting online information available; a process of *my search and research.*

words they used to run the search and which sites they visited. That information by itself seems irrelevant, but it is not.

For example, the search engine knows that an online user has a gardening interest because the user was searching for gardening centres; and the user may live in the London area, because the user also typed "gardening centres London". Then, the user might do a search about botanical gardens in Madeira. Soon after, the user may undertake another search looking for flights from London to Madeira. Shortly after those searches, the search engine displays to the user advertisements for hotels and flights to Madeira, and a subscription promotion of a gardening magazine which gives a welcome voucher for a workshop in the botanical gardens of Madeira Island.

Does this sound familiar to the reader? Most users have had this experience of being targeted by advertising online. Internet businesses are using cookies[37] and other technologies to track and profile users, and that can be a significant asset for their business models. Their stock market value relies on the unparalleled advertising revenue potential derived from accessing detailed personal information of a growing number of users in real time. This information collection and connection means that the user is not absolutely anonymous, since internet businesses can establish a profile, a "picture" of the user, though still a "nameless picture".

OSN like Facebook and Twitter allow users to interact and form an internet community where they can share significant amounts of information in real time. Individuals can choose to become a user, to post and select the information that they want to share and with whom, all for an "apparently" free service. At first sight, this seems a mirror of personal autonomy and ultimately democracy. However, the "consented" access which OSN obtain gives the service providers access to potentially much more valuable assets in the long term: users' online identity, profile and social behaviour information.

It may seem controversial to refer to anonymity within the Facebook and Twitter context, as some might argue that users of OSN do not seek anonymity when they engage on those social websites. However, we would question this over-broad assumption. Are users really consenting to allow those businesses to have unrestricted access to users' data? Do they reasonably expect that data to be disclosed, or even realise that it is possible to obtain its disclosure? Or is it more accurate to say, as we would suggest, that users believe they retain control over the disclosure of their information, and thus the degree to which their relative anonymity is compromised? The law is increasingly taking the user's side against OSN providers, in an attempt to reassert their rights of control.[38]

But although the law might be able to control the comparatively small number of organisations who have access to IP address information or operate OSN, it is likely to be powerless against the mass of internet users. The online world provides users with access to resources and information that were once only available to large organisations who were able to make significant investments in data collection. Today, with much less sophistication, any internet user also has access to enough resources and information to

[37] Cookies are data files sent from a website that the user is visiting and stored in the user´s web browser after access to that site. As such, every time that user accesses that same website through that same web browser, the website will know that the user has returned.

[38] For an overview see N Simmons, "Facebook and the Privacy Frontier" (2012) 33 *Business Law Review* 58-62, at 58.

uncover someone's identity, by collecting and connecting online data available; my search and research.

These resources consist of the search tools which have become an integral part of the internet, together with the significant amount of information that users make available online, consciously or not, and which is available to all other internet users; what we could call a "personal mind map". All information entered by users in their Facebook, Twitter, LinkedIn accounts and the information posted by companies or institutions with whom they are involved (photos, location, role) – the "digital dossier" according to Solove[39] – can lead to potential identification by anyone who is skilled enough to do a Google search, which in reality is the majority of us.

The MIT "Gaydar" [40] project demonstrated how it is possible to use Facebook links to establish the sexual orientation of users by analysing Facebook "friends" links. Users are likely to understand the public nature of the information they disclose expressly via OSN, but may not realise that this information can be analysed to discover undisclosed information which can be linked to their name. Users in the "Gaydar" project were expecting that their sexual orientation would remain nameless, and hence to some degree anonymous, but that expectation was false.

Online users have free access to infinite and worldwide information and it seems impossible, or even unthinkable, to control users' willingness to obtain information or knowledge in real time. Therefore, "my search and research" plays a significant role in attacking the core of anonymity and Solove's traceability concept.[41]

The fact that collection and connection of this personal mind map is available to the masses is a key difference from the data gathered by ISPs. Even though ISPs are able to gather large amounts of data, they do not normally voluntarily disclose users´ details, due to contractual confidentiality obligations and data protection laws. By contrast, the information that users freely enter and post online, therefore choosing to build their "personal mind map" and make it public, has a greater potential for interference in their lives, and even poses threats to the regular course of justice.

Recently, during the court proceedings of Oscar Pistorius' murder trial,[42] in which Mr Pistorius was found guilty of culpable homicide[43] of his girlfriend Reeva Steenkamp on Valentine's Day 2013, the judge restrained the media from broadcasting and using images of witnesses who requested the protection of their identity. However, while the first witness was giving evidence the court was informed that a picture of her was broadcast

---

[39] D Solove, "*The digital person: Technology and privacy in the information age*" (2004), New York: NYU Press.

[40] C Johnson, "Project 'Gaydar': At MIT, an Experiment Identifies Which Students Are Gay, Raising New Questions about Online Privacy" (20 Sept 2009), *Boston Globe* available at http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/ (accessed 1 Dec 2014).

[41] See note 33 above.

[42] Reported at BBC News website at http://www.bbc.co.uk/news/world-africa-26354615 (accessed 1 Dec 2014).

[43] Reported at The Guardian website at http://www.theguardian.com/world/2014/sep/11/oscar-pistorius-not-guilty-murder-reeva-steenkamp (accessed 1 Dec 2014).

by South African TV station eNCA[44] . The court immediately recessed to address the issue. In the meantime, Patrick Conroy, head of news at eNCA, informed the court that the image was taken from the website of the University where the witness teaches, arguing "that the image was publicly available and therefore did not violate the judge's order".[45] After consideration, the Judge concluded "that no photographs of any witness of any source should be broadcast", and made a strong appeal to the media, asking them to "behave".[46]

This case[47] demonstrates how judiciary and courts who promise to protect witnesses´ anonymity, as the law determines, can be unable to do so. The witness, who requested the court´s protection of her identity, had previously freely decided to make personal information public; and that information by itself led to identification. It is likely that the witness did not realise that such public information would be collected and connected by other users for different purposes and in different contexts. Nevertheless, it is undeniable that she decided, in an exercise of her autonomy, to make that information available to the public. By posting her "personal mind map" she, consciously or unconsciously, abdicated at least part of her anonymity because she can be named by a simple collection and connection of information available online.

The user's decision to disclose information in this way cannot readily be understood as being limited to the particular context where it was revealed. Such an approach would require the online searcher to identify the context of disclosure, and then accept an obligation not to use the information outside that context. Helen Nissenbaum´s argument[48] that privacy is "contextual", in the sense that it is always connected with the context in which it is revealed, might have been accurate for many real-world disclosures, but only because the disclosure took place in the context of some relationship between discloser and disclosee. Online disclosures are available to all, including those who have no relationship at all with the discloser. Thus, once a user decided to make information available online in a particular situation, and that information is available to the masses, the user cannot realistically expect not to be named in another different situation. A user who does not expect there to be such a risk has that expectation only because of their ignorance that the information they have made available to the masses, once connected, could potentially name them.

Identification through "my search and research" is a phenomenon which existing legal controls are ill-adapted to deal with. Court orders restraining identification are almost impossible to enforce against the general population as the Pistorius case illustrates.[49]

---

[44] Reported at The Time, http://time.com/12346/oscar-pistorius-neighbors-witness-broadcast-photo/ (accessed 14 December 2014).

[45] Ibid.

[46] See note 44 above.

[47] See notes 42 and 43 above.

[48] H Nissenbaum, *"Privacy as Contextual Integrity"* (2004) 79 Washington Law Review at 101-139.

[49] See also CTB v News Group Newspapers Limited [2011] EWHC 1326, where the court granted a superinjunction protecting the claimant's identity. However, soon afterwards his name was revealed worldwide by users of social networking site Twitter as part of a list of celebrities who sought superinjunctions.

In the Chedwyn (Ched) Evans' case his rape victim's identity was revealed on Twitter and Facebook just after conviction, *Regina v Chedwyn Michael Evans and Clayton Rodney McDonald* (2012) Caernarfon Crown Court. The law gives to victims of rape lifelong anonymity, and nine people were fined for

Data protection laws are designed to control the actions of large corporations, not individuals,[50] and data protection authorities have insufficient resources to pursue the mass of internet users. So far as "my search and research" is concerned there is real uncertainty whether data protection law would apply to the researcher, at least until the actual moment identification is achieved. As Lloyd points out:

> If an individual cannot be identified from the manner in which data is collected, processed, or used, there can be no significant threat to privacy and no justification for the application of at least the Data Protection Act—although there may well be rights under other legal headings such as the law of contract or the concept of breach of confidence.[51]

In this relative anonymity limbo, users' decisions about being anonymous or not and the expression of their consent to sharing information, is far from a simple "yes or no" option. It seems that autonomy is lost once a user consents to public disclosure, and from that point a user can only expect to be relatively, and contingently, anonymous.

3. Relative Anonymity and Courts

In recent years, courts have been asked to make orders about the disclosure of online identity information.[52] This is either via a court order to determine if in a particular case disclosure of users´ details should occur; or conversely the user seeks an injunction against a potential breach of his or her anonymity.

Their decisions[53] show that the courts are understanding that users are living in a relative anonymity limbo, while not explicitly acknowledging it. They are being asked to decide whether in particular cases users should be moved through the range of de-anonymization, and ultimately become named. The most important English cases here are the Sheffield Wednesday[54] and the "Night Jack"[55] cases. Those two cases also demonstrate that a decision about anonymity is not a "yes or no" option, but far more complex than that. What is clear is that the user's desire to be anonymous does not guarantee by itself an

committing contempt of court (The Guardian 5 November 2012, http://www.theguardian.com/uk/2012/nov/05/ched-evans-rape-naming-woman). But many others could not be identified, and the Crown Prosecution Service took the decision not to prosecute the operators of the website chedevans.com. in respect of pixelated CCTV footage of the victim (Sheffield Star 18 May 2015, http://www.thestar.co.uk/news/local/insufficient-evidence-to-prosecute-ched-evans-website-for-identifying-rape-victim-cps-rules-1-7266427).

[50] C Reed, "You talking' to me" in Dag Wiese Schartum, Lee Bygrave, & Anne Gunn Berge Bekken (eds.), *Jon Bing* A *Tribute* (2014 Oslo: Gyldendal Akademisk) 154.

[51] I Lloyd, "Anonymity and the law in the United Kingdom", in Kerr, I, Lucock, C and Steeves, V (eds), *Lessons from the Identity Trail* (Oxford University Press, 2009) 485, 487.

[52] *Sheffield Wednesday Football Club Ltd, Dave Allen, Keith Addy, Ashley Carson, Kenneth Cooke, Robert Grierson, Geoffrey Hulley, Kaven Walker v Neil Hargreaves* [2007] EWHC 2375 (QB); *Author of a Blog v Times Newspaper*, [2009] EWHC 1358 (QB); *Jane Clift v Martin Clarke* [2011] EWHC 1164 (QB).

[53] Ibid.

[54] *Sheffield Wednesday Football Club Ltd, Dave Allen, Keith Addy, Ashley Carson, Kenneth Cooke, Robert Grierson, Geoffrey Hulley, Kaven Walker v Neil Hargreaves* [2007] EWHC 2375 (QB).

[55] *Author of a Blog v Times Newspaper*, [2009] EWHC 1358 (QB).

enforceable absolute right to remain anonymous, nor even a reasonable expectation of remaining so.

In 2007, Sheffield Wednesday Football Club Ltd and its shareholders[56] asked the court to grant a "Norwich Pharmacal" disclosure order against Neil Hargreaves, who owned and operated a website called www.owlstalk.co.uk, on which fans of Sheffield Wednesday Football Club had posted allegedly defamatory messages. The claimant was seeking the identities of eleven users for the purpose of bringing libel proceedings. The website www.owlstalk.co.uk was freely accessible to anyone with access to the internet. In this case, the court analyzed whether each of fourteen posts were defamatory and, if so, whether the website owner should be ordered to disclose users' details. The court's decisions about disclosure depended on the seriousness of each post; i.e. the court defined a hierarchy of seriousness in relation to the content of the posts.[57] This hierarchy was used in balancing the posters' rights of privacy and free speech, which the court recognized would be impaired if their anonymity was broken, against the interest in disclosure.[58]

Comments classified with a low level of seriousness were those that were "barely defamatory", [59] "little more than abusive"[60] or "likely to be understood as jokes".[61] In these cases, the court decided that it "would be disproportionate and unjustifiably intrusive"[62] to individuals who made the less serious comments if information, which might lead to their identification, were disclosed. These were "website users who expected their identities to be kept hidden",[63] and the court recognized that it had a duty not to put that expectation of (relative) anonymity at risk unless there were strong countervailing reasons.

The highly serious posts, which led to disclosure orders, were those that would be likely to damage the club´s directors' reputation.[64] Such comments involved allegations of greed, selfishness, untrustworthy and dishonest behavior by the club's directors:[65]

> In the case of those postings, the Claimants' entitlement to take action to protect their right to reputation outweighs, in my judgment, the right of the authors to maintain their anonymity and their right to express themselves freely.[66]

Even if not expressly argued by the court, this decision highlights the relevance of articles 8 (right to privacy) and 10 (right to freedom of expression) of the European Convention on Human Rights and Fundamental Freedoms (EHRC) in deciding whether anonymity

---

[56] See note 54 above.

[57] Ibid.

[58] See note 54 above.

[59] *Sheffield Wednesday Football Club Ltd, Dave Allen, Keith Addy, Ashley Carson, Kenneth Cooke, Robert Grierson, Geoffrey Hulley, Kaven Walker v Neil Hargreaves* [2007] EWHC 2375 (QB).

[60] Ibid, (17).

[61] Ibid.

[62] See note 59 above.

[63] Ibid, (9).

[64] See note 59 above (18).

[65] See note 59.

[66] Ibid.

should be preserved. The court did not make a general assumption that all the fourteen posters of defamatory comments should have their identifying information disclosed. Even a wrongdoer was entitled to preserve their anonymity to avoid chilling their fundamental right of free speech, unless the wrongdoing was serious enough to justify the abrogation of that right. As such, the court decided that a level of seriousness of the post should be asserted in order to overturn anonymity[67] and also to achieve a proportionate balance between the rights of reputation, on the one hand, and privacy and free speech, on the other.

In this case, as soon as the users accessed the website www.owlstalk.co.uk they were no longer unidentifiable, because www.owlstalk.co.uk and their ISP knew some information about them. That information may not name them yet, but it can provide enough knowledge about those nameless persons so that they can be singularized from others and linked to specific online actions, as they were by a selection of comments among dozens. They were singularized within www.owlstalk.co.uk but they remained nameless – i.e. enjoying still some degree of anonymity – until the court's decision.

The *Author of a Blog v Times Newspaper*[68] case in 2009 caused outraged reactions by bloggers. The claimant, who was the author of a blog known as *Night Jack*, sought an interim injunction to restrain Times Newspapers Ltd (The Times) from publishing any information that would or might lead to his identification as the person responsible for that blog. That injunction[69] would restrain The Times from exercising its right of freedom of expression established in s.12 of the *Human Rights Act* 1998.[70] The Night Jack was a serving detective constable, and his blog mostly dealt with his police work and his opinions on a number of social and political issues relating to the police and the administration of justice.[71] He also criticised a number of ministers and cases where he had direct knowledge through his police duties.[72] The claimant was an anonymous blogger, who was claiming a "reasonable expectation of privacy" and arguing that there was no public interest to justify the publication of his identity since he had a legally enforceable right to maintain anonymity.[73] He also argued for a general "public interest of preserving the anonymity of the bloggers"[74] grounded on articles 8 (right to privacy) and 10 (right to freedom of expression) of *the European Convention on Human Rights and Fundamental Freedoms 1950* (ECHR).[75]

---

[67] In 2011 another case, *Jane Clift v Martin Clarke* [2011] EWHC 1164 (QB).

[68] *Author of a Blog v Times Newspaper* [2009] EWHC 1358 (QB).

[69] Ibid.

[70] Human Rights Act 1998, s 12: "Freedom of expression".

[71] See note 68, at (13).

[72] Ibid.

[73] See note 68.

[74] See note 68 above, at (5).

[75] See note 68 above.

The Times asserted[76] that it had been able to identify the claimant "(…) by a process of deduction and detective work, mainly using information available on the Internet (…)".[77] On that basis, the court denied the injunction on two grounds. First, "Night Jack" had failed to prove that the information had the necessary "quality of confidence" to be protected from disclosure as a breach of confidence.[78] Second, although persons are normally entitled to a reasonable expectation of privacy and thus protection against the improper disclosure of private information,[79] he could have no such expectation because blogging was "a public rather than a private activity".[80] Even if he was entitled to such an expectation, because "Night Jack" was a police officer his right of privacy "would be outweighed…by a countervailing public interest in revealing that a particular police officer has been making these communications".[81]

In this case, the "Night Jack" blogger started his process of de-anonymization once he setup the blog. He singularized himself by making all his postings on his blog, rather than posting them to different places using different pseudonyms. Finally, by the process of deduction and detective work, mainly using information available on the Internet, The Times newspaper was able to put a name to "Night Jack".[82] However, at this stage his identity was known only to The Times, and so he still had a degree of anonymity as against the rest of the world, which he could maintain if The Times was ordered to keep his name secret. Although the actual decision in this case is controversial,[83] the process of balancing competing interests in deciding whether to forbid disclosure is one which future courts will have to follow.

These two cases demonstrate how the courts will have to treat future cases where a "right" to anonymity is asserted. Where the anonymous communicator has been singularized, the question will be whether the internet intermediary which can name (or help to name) that person should be ordered to do so. If that person's name has been discovered through the process of my search and research then the question is different; should the court order

---

[76] This assertion may not have been accurate. On the 9th of October 2012, the press reported (http://www.bbc.com/news/uk-198851299) a settlement between Night Jack and The Times. Night Jack received a £42,500 payout from Times Newspapers after it emerged that a reporter on the paper unlawfully accessed his email account in a bid to reveal his identity in 2009.

The email hacking only came to light in January 2012 when Simon Toms and James Harding, referred in his Leveson inquiry witness statement to the incident available at http://webarchive.nationalarchives.gov.uk/20140122145147/http:/www.levesoninquiry.org.uk/wp-content/uploads/2012/01/Witness-Statement-of-Simon-Toms.pdf; http://webarchive.nationalarchives.gov.uk/20140122145147/http:/www.levesoninquiry.org.uk/wp-content/uploads/2012/02/Second-Witness-Statement-of-James-Harding.pdf (accessed 1 Dec 2014).

[77] See note 68 above, at (3).

[78] See note 68 above.

[79] On the basis of the right established in *Campbell v MGN Ltd*, [2004] 2 AC 457 and *McKennitt v Ash*, [2008] QB 73.

[80] [2009] EWHC 1358 (QB) para 11.

[81] Ibid, 19-29, but also see note 76 as to the accuracy of these facts.

[82] Ibid.

[83] E, Barendt, "Bad News for Bloggers" (2009) Journal *of Media Law* 1 (2) 141-147, at 146; L, Collingwood, "Privacy, Anonymity and Liability: Will Anonymous Communicators Have the Last Laugh?" (2012) *Computer Law & Security Review* 28(3) 328–334; E, Steyn, and S, Harrower, "Case Comment: Author of a Blog v Times Newspapers Ltd: Bloggingean end to Anonymity?" (2009) *Entertainment Law Review* 20 (8), 298 -299, at 299.

the name to remain secret? In either case, the court has to balance the public interest in naming the communicator against that person's individual rights of privacy and freedom of expression. And the court further has to decide how far to decrease the communicator's relative anonymity; in the *Sheffield Wednesday* case those posters who were ordered to be named were identified only to the claimant, whereas in the Night Jack case the naming was to the whole world.

4. Autonomy and consent

In real space, the maintenance of anonymity is a matter of autonomy.[84] You have a choice whether to identify yourself, and if you choose not to do so then in most cases that choice is effective. Admittedly, your real space anonymity is still relative, as the example of Van Gogh's *Sunset at Montmajour* shows, but, because it requires expensive research to identify you, the risk to your autonomy is low.

By contrast, in cyberspace you lose that autonomy because in order to communicate at all you have to consent to someone, usually at least your ISP and probably one or more OSN providers, knowing who you are. Further, in the terms and conditions of service to which you signed up, you agreed to allow the provider to disclose your identity to others.[85] Even if your service provider agrees to limit identity disclosure to the minimum permitted by law, by communicating online you inevitably open yourself to the possibility of identification via my search and research. Until comparatively recently it was possible to argue that cyberspace communicators would maintain their autonomy by choosing the information that they would disclose,[86] but today the sheer volume of information available for "my search and research", coupled with the sophistication of the tools available for that purpose, renders this exercise largely futile.

The most recent legal development in this area appears to be an attempt to restore at least some of that lost autonomy to cyberspace users. In May 2014 the CJEU gave its judgment in *Google Spain v AEPD*[87] in which it upheld the decision of the Spanish data protection authority and the Audienca National (National High Court) that a data subject had the right to request search engine providers such as Google to remove personal data from search results. The claimant had asserted that news reports dating

---

[84] See notes 10 and 15 above.

[85] The extent of permitted disclosure varies widely. BT's Broadband terms permit disclosure in accordance with its Privacy Policy, which limits disclosure to lawful requests from law enforcement agencies and others, such as rights owners available at http://home.bt.com/pages/navigation/privacypolicy.html?page=Broadband. Facebook's terms incorporate its Data Use Policy available at https://www.facebook.com/about/privacy/your-info, which permits disclosure far more widely. The Policy is completely silent on the question of law enforcement access, which is dealt with by a separate set of operational guidelines, which are not expressly contractually binding on Facebook: available at https://www.facebook.com/safety/groups/law/guidelines/. There appears to be little consistency between service providers in relation to identity disclosure (accessed 1 Dec 2014).

[86] Thus as recently as 2009 Lloyd could argue:

> It is fair criticism that too little has been done to create a framework for a right of anonymity, but all too often people fail to take even the most elementary steps to protect themselves.

I Lloyd, n 51, 502.

[87] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12 [2014] ECJ.

from 1998, relating to a debt recovery action, were no longer relevant to him because the dispute had long been resolved, and thus their processing by Google contravened the data protection principles of Article 6 of the Data Protection Directive.[88] The CJEU confirmed that the Directive did indeed grant such a right:

> "… even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed".[89]

This "right to be forgotten", which it appears was already implicit in the Directive, has proved as controversial as the proposal to introduce it in the draft Data Protection Regulation.[90] Google has set up a process for receiving and deciding on requests, and is applying exactly the same kind of balancing between private and public rights which we saw in the UK courts decisions examined in part 3 above. Data protection authorities and commentators are already finding fault with the process,[91] and concerns are being raised about whether the right properly balances the public interest in matters such as removing information about criminal convictions for sex offences.[92] It begins to look as if the autonomy to *remain* anonymous is conceptually different from the autonomy to *become* anonymous once one has previously been named.

Conclusion

In cyberspace, anonymity is both relative and ephemeral. The effectiveness of an initial decision to act anonymously depends on your relationship with third parties and the disclosures you have consented to. That anonymity is contingent, constantly at risk from my search and research activities. But, most importantly, that decision is not one for the cyberspace user alone. The decisions of service providers, regulators, courts and other cyberspace users are equally significant, and in many cases unpredictable. Anonymity might be desirable for many cyberspace users, but as the song says, ***You Can't Always Get What You Want.***

---

[88] Ibid, 72.

[89] See note 87 above, at 93.

[90] Personal data protection: processing and free movement of data (General Data Protection Regulation), available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 1 Dec 2014), see also European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN (accessed 1 Dec 2014).

[91] See "Google Jogs Memories Meant to Be Forgotten, Watchdog Says", *Bloomberg Business Week* 24 July 2014 available at http://www.businessweek.com/news/2014-07-23/google-jogs-memories-meant-to-be-forgotten-watchdog-says (accessed 1 Dec 2014).

[92] See eg 'Dishonest calls on 'right to be forgotten' may be hiding crimes', *The Times* 1 August 2014.