Chapter 13
ANONYMITY: CHALLENGES FOR POLITICS AND LAW

Chris Nicoll and Corien Prins

We started with the observation that some commentators consider appeals to anonymity to be little more than rhetoric and not worthy of serious consideration. This book takes a completely different perspective. The authors of the different chapters have shown us that the concept of anonymity is increasingly invoked in the information society debate and that this development gives rise to various questions, dilemmas and fields of tension. This final chapter intends to draw tentative conclusions concerning the dimensions of anonymity and how it is defined differently depending on its context. It then discusses the tensions or conflicts in the differing values and, finally, elaborates on the approach the law is taking and may take in the future.

1. The Concept of Anonymity

The first question that arises is whether the discussion in the previous chapters leaves us with a common denominator of "anonymity". What is anonymity? The dictionary meaning of "nameless" does not take us very far. Is it an absolute or a flexible notion? Grijpink and Prins observe that we are not anonymous to ourselves but we can be anonymous to others if they cannot discover who we are or could only do so by disproportionate effort. This suggests that anonymity is dependent on the perspective of the viewer. It also introduces the idea that to be known by one person does not necessarily negate anonymity as far as others are concerned. Perhaps in this latter respect one could say that it is a resource or quality that is renewable by virtue of the fact that human memory depreciates with time. So it has a temporal dimension.

If we are not anonymous to ourselves, anonymity cannot be an absolute notion. It must be a state that describes identity, a matter of degree, a point or section on the broad spectrum of identity with identity being, as Deighton states: "... a set of characteristics by which someone is recognizable or known, and while identities may change the changes occur slowly because they reside as much in the memory of the observer as in the intention of the actor".

C. Nicoll, et al. (Eds), Digital Anonymity and the Law – Tensions and Dimensions

But at what point on the identity spectrum does anonymity reside? Grijpink and Prins talk of "absolute anonymity" and "semi-anonymity" in the context of a "transaction". Absolute anonymity is where no traces remain to establish identity. Semi-anonymity is where some traces remain and, within that category, they discern further degrees dependent on identity knowledge of some third party to the particular transaction. They also make the interesting point that a viewer may not necessarily be interested in a *name* as an ingredient of identity but may be interested only in qualification or status against the background of a particular transaction. For example, a cash deposit to load a PIN protected chip card that can then be used to buy goods. In such a case the trader is not concerned with enquiring who the purchaser is, she only cares that the card has a sufficient credit balance and that two attributes (PIN and card) coincide in the one identity. This process falls short of "identification" in the authors' terminology; they term it as "verification".

So from this we can draw the tentative conclusion that anonymity, because there would seem to be degrees of it in practice, occupies a *section* of the identity spectrum that may be influenced by the nature of the particular transaction. The lesson to be learned here is that anonymity is multi-faceted; the way we look at it depends on the context within which we are working and the goals we seek to achieve. But if anonymity exists at one end of the identity spectrum, what lies at the other end? Obviously it is the state where one's identity is completely revealed. As we have seen (Deighton), there are advantages to the individual in having control over both ends of the spectrum: anonymity and identification. Indeed, in the commercial context it may be that the answer is to empower the data subject by appropriate mediation, within a market model, between situations that, on the one hand, allow the opportunity to purchase anonymity and, on the other, allow the subject to profit from the use of identifying information by others.

At this point, it is useful to observe that anonymity is not the sole preserve of lawyers and lawmakers. It is the concern of computer scientists, software engineers, marketing experts, copyright proprietors and others. This is because it is a state that is distinct from the law. A lawyer from a common law jurisdiction would describe it as a question of fact as opposed to a question of law. In any given situation a person occupies a given point or section of the spectrum. It is only the measures by which she attempts to retain her anonymity and the means adopted to exert her identity that are influenced by legal and societal pressures. Technology will develop on two fronts as it has done since time immemorial. It will refine existing tools and invent new methods to, on the one hand, conceal identity and increase the security of communications, and, on the other, to reveal and detect identity and decode secret messages.

Because the notion of anonymity is multi-faceted, it is unlikely that any consensus will be achieved to bring about legislation against the *development* of the technology. The law has never triumphed for long over the march of scientific enquiry particularly when the immediate uses to which new inventions can be

put are unclear.[1] But the law does have a role to play where societal pressures and the interests of the State are affected by the erosion of privacy. Here we broach the subject of "rights". What do this book's contributors teach us with regard to the relation between anonymity and privacy?

2. Anonymity and Privacy

When reading Deighton's analysis, we note that here privacy is equated with anonymity: "privacy is not the absence of identity, but rather a state in which identity is masked or undetected". Privacy can, however, also be distinguished from anonymity. While anonymity is a state of being, privacy is the degree to which a member of society chooses to employ that state of being in his or her interactions with the State and with other citizens. As Howells and Edwards observe, there are even categories of privacy: corporeal, of property and possessions and informational although it is the last which is of principal relevance in this book.

The degree of privacy one chooses to exercise may be a matter of personality or preference alone. "Masks are needed to consult the heart and to allow for some leeway in conforming to role expectations."[2] Anonymity may be a "shield from the tyranny of the majority".[3] It does not always facilitate wrong by eliminating accountability. But it can be used to achieve specific purposes not otherwise achievable – some of those purposes may lack social utility and may even be contrary to the law. The choice exercised by the citizen is, as we have seen, one that has changed in degree as society itself has changed. In classical times nascent democracies were small and depended for their survival, as a form of participatory government, on active involvement by each member. Those who did not subject their personalities to full public gaze were viewed with suspicion. Perhaps they were regarded as a member of a team who did not "pull his weight"?

With the passage of time city-states grew into the metropolis and small towns became larger towns sometimes resulting in the conurbations of the 19th and 20th centuries. Geographical, cultural and language propinquity resulted in the formation of nations and of national groupings. These modern structures did not and do not now permit or encourage the same degree of participation as in former times – in some cases, of course, participation is forbidden to all but a few. In these situations, the degree of privacy considered appropriate by those such as Jeremy Bentham, tended to be at the restrictive end of the scale – but for a differ-

---

[1] For example, number theory had little practical application until the Second World War brought about advances in cryptographic techniques.

[2] De Hert referring to J. Silber's 'Masks and Fig Leaves', chapter 3, n. 5.

[3] *McIntyre* v. *Ohio Elections Commission,* 514 US 334 (1995) at p. 357.

ent reason than may have been the justification in the city-state of the 5th century BC. Privacy was inimical to social control. Bentham's idea of tattooing a unique number on the person of each citizen would be viewed with horror today. Yet if we put aside the precise technology he suggests, it is an idea that differs little in principle from calls in the United States for national identity cards.[4] As De Hert states: "Some of Bentham's proposals to permanently citizens' anonymity sound very rude to contemporary ears, but, with the advent of softer techniques, they may become a desirable reality for some."

The softer techniques to which he refers may make such measures more palatable but also events of geopolitical importance, such as heightened terrorist activity, may have a similar effect that outlasts the immediate cause of the resulting restriction. Structures and bureaucracy to deal with a short-lived crisis may, as Constant observed, take on a life and vigour of their own becoming self-perpetuating and aggrandizing – organize a secret service and conspiracies will be found everywhere.

If, therefore, we regard privacy as the degree to which a member of society chooses to employ anonymity or various degrees of anonymity in daily life, it can be seen that that choice is bound to become subject, to a greater or lesser extent, to the greater good of or the *perceived* well-being of the State. Indeed, because an individual's choice is bound as a practical matter to be arbitrated to some extent by the State, an alternative construction is to regard privacy not so much as a matter of choice but as a matter of the legal boundaries and limitations within which that choice can be exercised. Or, as Katsh puts it: the *power* to control what others can come to know about you. But whatever construction one elects to adopt, it is the extent of moderation in the light of existing and future technologies, in particular in their ability to enhance or reduce anonymity, that gives rise to modern-day problems.

3. Anonymity and Contracting

While the main thrust of this book is anonymity in the digital world, it should not be forgotten that the use of anonymity and various points along the continuum culminating in that state are not confined to the electronic medium. It has been noted that contracts can be made with one or even both parties being unaware of the identity of the other. Examples being the automatic drink dispenser or the confectionery machine, the pay-as-you-leave carpark, and even the sale of travel insurance at airports.

Impediments to anonymous contracting tend to be practical rather than legal. For example, if one does not know the identity of the other contracting party there is no effective recourse against that person if the contract is broken and

[4] See Froomkin, chapter 2.

damages are suffered, vendors will not be secure in providing delivery if they cannot see a clear path to receiving payment. But there are legal structures that can be used to satisfy these concerns while still ensuring the privacy of the participants. As Grijpink and Prins point out, there is the trust, there is the principle of agency where the agent is either undisclosed or unidentified. It is also possible to transact business by using an intermediary such as a company or an association. The point here is that anonymity in business or in contract is not a new concept and is generally untrammelled by legal requirements except in distinct areas that arise from some special character, frailty or vulnerability of one party, for example, persons below the age of majority or consumers. As the UNCITRAL Working Group on Electronic Commerce discovered in early research eventually leading to the Model Law on Electronic Commerce 1996, there are few jurisdictions where contracts must generally be evidenced in writing although there are some categories of contract, commonly those for the sale of land, that must. With respect to the international sale of goods to which the Vienna Convention applies – and this represents the preponderant volume of world trade – there are no form requirements. However, the advent of the Internet, cryptographic techniques, etc., have added a new dimension to the old anonymizing mechanisms. Anonymous communications have been facilitated by the new technology. Yet they may be employed *in conjunction* with the old legal constructions. The whole may prove to be greater than the sum of these two parts.

4. Tensions

Everyday life is evidence that technological advance provides for numerous opportunities to trace and track people down. However, the possibilities for anonymous communication are enhanced by new technologies as well. Thus questions, dilemmas and fields of tension arise. Where does one draw the line between anonymity as a tool, on the one hand, for citizens to protect their civil and constitutional rights, privacy and other interests and, on the other, identification as an instrument in criminal investigation, commercial marketing, social control, etc. Here we see many tensions. To provide just a few examples, there are the tensions between:

- Anonymity and privacy *contra* intrusions to detect or forestall crime (crime detection being one form of identification). As Carr describes, the Council of Europe Convention on Cybercrime attempts to grapple with substantive criminal law, evidence, procedure and general principles for international co-operation.
- Anonymity and privacy *contra* intrusions in the interests of national security for which we have illustrations in the chapter by Goemans and Dumortier.
- Privacy *contra* financial and other benefits from giving up some privacy or

tolerating some annoyance in one's daily life[5] as described by Deighton.

- Privacy as an aid to free speech and dissent in the political context *contra* privacy as a mask for socially undesirable speech such as defamation – these matters being introduced in the United States context by Froomkin.
- Completely anonymous data *contra* data that is personal for the purposes of data protection legislation. This topic has been discussed by Walden in the medical context in the light of the decision of the United Kingdom Court of Appeal in *R* v. *Department of Health, ex parte Source Informatics Ltd* and includes the balance to be struck between the interests of researchers who use personal data as part of their raw material and the interests of data subjects – particularly where the latter's data have gone through an "anonymizing" process.
- Visibly collected personal data *contra* invisibly collected data. This tension is particularly apparent in the relationship between traders and the consumer. Howells and Edwards discuss the different grades or levels of privacy in this area and lament the present lack of discretion and flexibility of the consumer when it comes to managing the use of his own personal data. The system does not accommodate any subtlety in his exercising informed consent.

In each case a balance must be achieved by the law in the light of contemporary policy considerations and, of course, there will be ebb and flow with respect to these considerations as circumstances change – and change they will, often quite rapidly.

However, perhaps the greater concern of lawmakers will be changes in the technology itself. It can be argued that the debate about anonymity and privacy (both off-line and on-line) has been stimulated not so much by a general policy change such as individualism versus republicanism but by the simple fact that computers can now provide cheap communication, economic storage of data and reliable data retrieval. For example, there is concern about surveillance cameras in public places. There have always been spies in public places. There have always been observant people in public places whether they have a special reason to be observant such as the shopkeeper who looks to see what his customer's special and individual preferences are or whether they are simply entertained by the activities of their fellow man. The difference today is that face recognition software along with data retrieval methods and low cost data storage devices can exceed in a day the total efforts of every spy ever employed.

The same applies in the commercial context. As Deighton observes, the history of business can be read as a history of improvements in matching supply to demand. In some industries, such as banking, where revealing data about a customer's proclivities is a by-product of service delivery, enormous efficiencies

[5] ' ... telemarketing phone calls at dinnertime, trafficking in medical information, spam e-mail, pop-up Internet advertisements and other pesterings'.

were obtained particularly where data was pooled between ostensible competitors. These efficiencies were not previously available where such by-products did not exist but, because of the information technologies (databases, call centres, the Internet, etc.), matches between products and individually identified customers can now be achieved. In the process of achieving these efficiencies, of course, the customer's privacy is compromised although he does attain some countervailing benefits.

As a final illustration, the direct influence of the technology on the societal, and ultimately the legal, issue of privacy can both create problems and solve them. Some of the difficulties confronted by the UK Regulation of Investigatory Powers Act 2000 and a similar Belgian legal provision requiring the retention of traffic data[6] may be reduced when the Internet Protocol IPv6 is in wider use. Changes in the global routing architecture will also have an undoubted effect on the need for laws that call for storage of traffic data (with the high administrative overheads such provisions involve).

So the changing technology has a direct influence on the law – an influence of the same or of a greater magnitude than experienced with the railways and the telegraph system. Yet it would be unwise to restrict the legal inquiry to appropriate reactions to the changes the technology has brought or will bring about. The related subjects of anonymity and privacy deserve separate analysis because their underlying principles are important and have always existed; albeit they have only achieved notoriety through technical innovation.

5. Striking a balance

At the present time no consistent policy can be discerned in any one jurisdiction that would allow the resolution of the tensions illustrated *above*. Each problem relies on striking a fair balance between the interests of the individual on the one hand, and the interests of the State on the other. Alternatively, a balance must be struck between the interests of the individual (commonly the consumer) on the one hand, and the interests of the market on the other – all the while cognizant of the fact that an efficient market benefits the public as a whole.

What can be the role of privacy rights in striking a balance? We note here that the law in the general area of privacy is developing in separate "islands". Indeed, it is clear that there is no bridging, unqualified right to privacy at all although something approaching an unqualified right appears to exist under Austrian data protection legislation in the narrower area of *personal data* concerning the individual citizen.[7] For instance, Article 8 of the European Convention on Human Rights and Fundamental Freedoms gives a right to *respect* for a citizen's private

[6] See Goemans and Dumortier, chapter 8.
[7] See Walden, chapter 7.

life, his home and his correspondence. But the flexible notion of "respect" is informed by the interests of national security, public safety, the economic well-being of the country, prevention of disorder and crime, protection of public morals and the rights and freedom of others. The discussion by Goemans and Dumortier shows how difficult it is with traffic data to reconcile the citizen's privacy with these societal values and Froomkin mentions FCC rules that require certain identifying information to be provided in the case of facsimile communication.

In the United States there is no express right to privacy guaranteed by the Constitution. There, the recognition of the need for citizens to be able to communicate anonymously is derived from the right to speak freely, to dissent and criticize, to associate freely, to play a full role in the democratic process. Furthermore, the boundaries are being extended to include a right to read anonymously. However, these rights are not absolute as they are, like their European counterparts, subject to a compelling government interest especially where no alternative regulation can achieve the legitimate public interest goal.

Clear guidelines seem only to exist in the political context. Commercial interests are accorded reduced protection. There is no equivalent of the express reference to the economic well-being of the country as exists in the European Convention on Human Rights and Fundamental Freedoms. It may be that the market will regulate itself. That may be through compromising or the "spending" of privacy which becomes tantamount to an asset. The countervailing benefit is some form of financial gain as described by Deighton. The market may also regulate itself through a professional body or association. But here, as illustrated by Carr in connection with the Internet Watch Foundation, a private association may effectively block the door to the Internet or restrict permissible activities in the absence of any public debate or even in direct opposition to public demand. The danger of this sort of private intervention is that it may often occur because the trade body concerned fears government regulation. The government is able to abdicate its responsibilities in a politically unproductive or dangerous area by permitting a form of delegated legislation while avoiding any accountability.

Yet fundamental to the regulation of anonymous Internet activity is the recognition that communication is not "geographically contained".[8] The nature of the medium dictates that the detection and prevention of Internet crime for example, must be accompanied by a degree of international co-operation that has not so far been possible to attain in other contexts. Not only is it difficult, owing to cultural and political differences, to reach an international consensus on a list of alleged crimes that would justify a co-ordinated approach in their detection, but the process is further exacerbated by wide dissemination of evidence, the transient nature of much of the evidence and a trail that quickly turns cold.[9] It has

[8] See Carr, chapter 9.

[9] A problem which is not assisted where there are large time differences between the relevant countries.

been observed (Sims) that various procedural means are available in common law countries to gain the courts' assistance in breaking through identity barriers. Yet these methods can be hampered by a lack of formalized transnational co-operation. The transnational nature of the Internet is not only a problem in securing a uniform approach to on-line anonymity. Arguably (Howells and Edwards) it gives an unfair advantage to lobby or interest groups who are able to band together and thereby to focus attention on influencing legal developments to their advantage at the expense of less cohesive or numerically manageable interests such as consumers. Ironically, it is consumers who are the major driving forces in the growth of e-commerce. Yet surveys have shown that they have little confidence in the medium, an attitude that is, perhaps, disproportionately affected by invasions of privacy such a spam and junkmail which, whilst they do little economic harm, can cause huge annoyance and sometimes emotional distress.

6. The Future

The *above* shows us that there is no definite guideline to determine the boundaries of anonymity and the interests that determine whether and to what extent limitations on anonymity are required or not. Generally speaking, the different chapters in this book show us that the limitations on anonymity can be said to reflect the courts' or the legislator's recognition of various interests (criminal investigation, national security, etc.) in making a person's identity known. It also shows us that there is no such thing as an absolute right to anonymity. The question then arises: if limitations on anonymous communications and transactions are considered to form an integral part of balancing individual and societal interests, can something be said about future developments that may influence this bargain? It will be clear that the answer to this question depends on various factors. For one, the answer will vary from one country to the next, since countries each have their individual approach to considerations such as the principle of freedom of expression, the interests of national security, etc. Another factor that influences the answer is changing technology, posing new threats to anonymity.

This book has shown us that advances in digital technology have provided public agencies, organizations and companies with the opportunity to develop new ways of revealing information on people's identity. There is no doubt that the advance of the digital age will also enhance the possibilities of tracking and tracing by private individuals. The development of intelligent agent technology could bring with it a huge potential for intelligent ways of tracing and tracking people. Intelligent agents are characterized in that they should be autonomous, proactive, reactive and sociable.[10] They do not rely on explicit commands of a

[10] The first property (autonomous) means that the agents should be relatively independent in executing their functions. The last property (sociability) has as consequence that an agent should be

user and are able to collect and filter in an intelligent manner an enormous amount of identity-related information as well as to guide and monitor long-term communication and transaction processes of people on the Internet.

At the moment agent technology is not a particular threat because it only automates what can be done manually by web-browsing and it can be blocked automatically. But it could become a new threat to anonymity when widely available and may, indeed, gain the ability to respond to its environment in an intelligent and proactive manner – exhibiting social abilities. It is precisely by these abilities that intelligent agents can take on a life of their own, replicating human-based communication and interaction. Certain actions in tracking and tracing identity-related information on the Internet could become totally independent of day-to-day supervision by human beings. On the other hand, there is no doubt that agent technology itself can become an instrument for the protection of the anonymity interests. As with many other applications of ICT the maxim "the answer to the machine is in the machine" applies. By means of their agent, individuals could make known and control the circumstances under which they want to reveal or hide their identity.

Another digital application that could bring potential for balancing anonymity and the quest of governments and businesses to have identification data available, is the facility of Trusted Third Parties; among them Certification Authorities. They could play an intermediate role in keeping a true identity secret, but also in providing identity and tracing information once certain conditions are satisfied. Of course, there will be continued debate (as in France and the UK) over whether they must retain in escrow identifying information in the event that governments require, ostensibly for state security reasons, to decrypt messages. In line with present developments in the US with internet service providers having to reveal the identity of people posting information through their facilities, case law, self-regulatory initiatives and maybe even legislation may set the conditions under which identifying information must be revealed by intermediaries. Of course there are drawbacks in third parties becoming involved in this area. We note that there is a move towards Certification Authorities granting recognition to other certification authorities. If this involves widespread combining of identifying information such a private keys, it will have serious implications. First, if such information is combined internationally, the databases will become very attractive targets for hackers. Secondly, individual states may find that their ability to protect the privacy of their own nationals is lessened. In other words, there may be a reduction in national sovereignty.

---

able to communicate with its environment and is able to co-operate with it (including other agents). This means that the actions of an agent can be influenced by other agents. The property of proactiveness means that agents have their own (in-built) goals that they try to achieve. Therefore they do not rely on explicit commands of a user to start operating. Finally, the reactive character of agents means that they can react to changes in the environment.

A final remark relates to the *spectrum* with anonymity at one end and identification at the other and the apparent belief that one has revealed someone's identity.

First, there are various degrees between the extremes of the spectrum. People often claim they need to identify someone, whereas in fact it would be sufficient for them merely to ensure that identifying data coincides with the same person without the subject's true identity being uncovered. Therefore, in balancing between anonymity and identification, policy-makers, the courts and scholars should not fail to address the distinction between identification and verification.

Secondly, we should be aware that our identity has become a prime example of the new virtual vulnerabilities. With the advent of the on-line world and the new possibilities of digitizing identity-related characteristics, the ways of identifying individuals are increasing.[11] This book shows various newly introduced concepts, such as virtual identity, pseudonymity and anonymity and these digital and multiple identities created may feed back into the off-line world, offering a mix of physical/virtual plural identities. Also, the reasons for introducing and using virtual identification methods are many and varied – they may be created for reasons of security, profit, convenience or simply fun.

Another vulnerability related to the on-line world is identity theft, being at present one of the fastest growing crimes in the United States.[12] But problems arise not only because criminals have access to unique identity tokens. A key problem in our present-day society is also that government organizations and companies rely on identification but lack a truly accurate digitised means of identification. This explains the growing demand for digital methods relying on biometric and DNA imaging technology that trace a unique person, so it is said, with absolute certainty. However, the introduction of these new invasive methods based on bio-dynamics, retinal scans, DNA patterns and other unique physical characteristics has caused debate and controversy. The key challenge now is to make the new models for identification and identity management compliant with anonymity, privacy and other societal and ethical standards. Identification has become a concept with multiple variations, forcing policy-makers, the courts, private organizations and others to rethink and redefine identity, identification interests and the mechanisms for identification. But in the end they must be offset against and balanced by anonymity.

---

[11] The new digitized identification methods can be divided into numerous categories. There are physical-based characteristics (biometry, DNA) and knowledge-based mechanisms (password, PIN code) and token-based methods (chip card, and other carriers of identification characteristics). There are intentional (typing of a code) and unintentional methods (camera); active and passive methods, etc.

[12] The US Department of Justice reported a case in which someone was found trying to sell 1,000 social security numbers for $1 each on eBay. For this and other examples, *Electronic Commerce & Law Report*, 8 May 2002, pp. 434-435.