PART III

ANONYMITY

Building on our investigation of the various concepts and technologies pertaining to identity and identification in Part II, Part III offers a snapshot of the laws governing our ability or inability to be anonymous. Scholars from five North American and European jurisdictions—Michael Froomkin from the United States; Carole Lucock and Katie Black from Canada; Ian Lloyd from the United Kingdom; Simone van der Hof, Bert-Jaap Koops, and Ronald Leenes from the Netherlands; and Giusella Finocchiaro from Italy—survey the place of anonymity across the legal domain and assess the law as it currently stands in each country. Although each survey can be read in isolation, it is interesting to consider some of the similarities and differences among and between them.

No "right to anonymity" is explicitly protected by any of the five jurisdictions' constitutions or human rights provisions. However, anonymity may enjoy limited protection as an acknowledged component of another right or freedom, in particular, privacy, freedom of expression, restrictions on state search and seizure, and provisions related to protecting liberty and life. In fact, it would seem that there is no coherent or integrated approach to anonymity in any jurisdiction. Rather, the law has developed piecemeal in a number of disparate public and private law areas. Consequently, the meaning of anonymity is contextually situated and may vary from one area of law to another.

All in all, each jurisdiction reports scant protection of anonymity, a preference for identifiability, and an increasing encroachment on areas of de facto anonymity that the law, to date, has not protected. Each author discusses the law's specific responses to the network society along with descriptions of existing approaches to anonymity in a broad range of areas within their jurisdictions. Despite differences, there is a great deal of similarity to the legal approach in each country, aided perhaps by adherence to or influence of international agreements, treaties, and directives. In addition, legal protections for anonymity in all five jurisdictions appear to be shrinking, as the focus on safety and security has repeatedly trumped the call or justification for anonymity.

For example, each jurisdiction has considered a requirement to carry a national identity card, and this has created prominent debate in most. The introduction of an all-purpose identity card is a significant change that promises to have a chilling effect on anonymity. This has been presaged in some jurisdictions by judicial decisions that have lowered the threshold of the legal grounds necessary for law enforcement personnel to detain persons and to require them to identify themselves. Even when a national identity card has not been introduced, a number of jurisdictions have added biometrics and radio frequency identification chips to "smart" drivers' licenses, in effect turning them into de facto identity cards.

Apart from a general requirement to identify oneself to the state, each jurisdiction reports instances in which identification is statutorily required. Examples include producing a driver's license when using public highways and providing identifying

information in order to conduct banking transactions. Courts and tribunals have similarly upheld requirements that individuals identify themselves for certain commercial purposes such as obtaining a refund or exchanging goods. In all jurisdictions, there has been an increase in these calls for context-specific mandatory identification and a consequent reduction in the ability to transact or enter commercial or noncommercial relations anonymously.

The use of surveillance in public spaces, particularly video surveillance, is clearly increasing in all jurisdictions. The de facto anonymity once enjoyed in these spaces has, as a consequence, diminished, and to date the law seems to be enabling the deployment of technologies of surveillance rather than protecting anonymity.

The appropriate role of and the degree of control over the providers of communications services, especially Internet service providers, is another area in which the law in currently in flux. The combined interests of law enforcement agencies and the private sector in ensuring that identity can be revealed on demand has resulted in significant pressure to require service providers to collect and maintain records for identification purposes and, in some countries, to allow identifying information to be disclosed to authorities without judicial preauthorization or oversight.

Although there are remarkable similarities in approach among the five jurisdictions, there are also some interesting differences. For example, the United States reports that a strong adherence to the open court principle has limited the use of a pseudonym in criminal and private law proceedings. This is in stark contrast to other jurisdictions where the use of a pseudonym is supported both by the courts and by legislation as a means to protect and promote the pursuit of legal claims. Although in these jurisdictions the use of a pseudonym and a publication ban does not usually shield facts or the identity of witnesses from an accused, there are exceptions. In Canada, undercover operatives may have their identity concealed, and in the United Kingdom, recent legislation now permits the granting of witness anonymity orders to protect the witness's anonymity. Interestingly, Canada also reports that permission to use a pseudonym to protect privacy may now be given to those persons who have used an online pseudonym to enable them to continue to use it in court.

Other differences are equally noteworthy. The UK law enforcement DNA database has been particularly controversial, especially given its size and the wide set of circumstances that allow the government to add information to it. Although other jurisdictions have similar databases, the restrictions on information inclusion and use appear far more stringent. The Netherlands reports growing concerns over electronic voting, including the use of the Internet for remote balloting. As other jurisdictions contemplate or implement e-voting, many wonder how the traditional protection of voter secrecy and the assurance of system integrity and accountability will be preserved and protected. Italy reports

a number of interesting provisions that legally protect the right to be anonymous in some circumstances, including entering a detoxification center, seeking help for social problems, and protecting the name of the mother at the time of childbirth.

Each author expresses a general concern as to the direction the law is taking and calls for greater attention to and protection of anonymity as a necessary component of protecting valued human rights such as liberty, dignity, and privacy.