

Ian R. Kerr
Canada Research Chair in Ethics, Law & Technology
Faculty of Law : Faculte de droit
Common Law Section : Section Common Law
University of Ottawa : Universite d' Ottawa
57 Louis Pasteur St., P.O. Box 450, Stn.A
Ottawa, Ontario K1N 6N5
t 613.562.5800 ext. 3281
f 613.562.5124
iankerr@uottawa.ca
www.ANONequity.org
www.blogonymity.info

Anonymity

Historically, the concept of anonymity was associated with a state of namelessness. Being an *anonym* afforded certain advantages. It enabled the nameless to speak without fear of reprisal, or to engage in acts of charity or other forms of benevolence. At the same time, it made possible wrongdoing without accountability.

With the advent of computer based communications networks, there has been a resurgence of interest in the nature and value of certain types of anonymity. The range of techniques by which individuals are able to operate *incognito* creates a virtual laboratory for experimenting with the social construction of identity. However, as the internet's surveillance potential becomes better understood and exploited, the measure of one's anonymity shifts from its historical focus on names to a broader investigation of a range of personal identifiers that can be linked to an individual. These include: date of birth, marital status, social security number, passport information, property ownership, vehicle registration, driver's license number, facial characteristics, height, email address, place of business, phone number, credit card history, iris shape, fingerprints, retinal image,

employment record, blood chemistry, roadway usage, gait pattern, consumer purchases, Google search history, internet protocol address, and the like.

Unbeknownst to many, the increasing ability to link these identifiers to an individual has resulted in a diminished ability to maintain anonymity, resulting in applications for subpoenas and court orders requiring third parties to disclose identifying information for the purposes of private lawsuits or police investigation. In light of the numerous possible identifiers in an information age, anonymity is perhaps best understood as a state of disconnection between one's self and one's identifiers; a state in which data cannot be associated with a particular individual, either from the data itself, or by combining it with other data. The value of anonymity, as Nissenbaum has put it, lies not in the capacity to be unnamed, but in the possibility of acting or participating while remaining unreachable.

Anonymity's 'unreachability' provides one means of achieving Westin's conception of informational privacy: people who are able to disconnect their identities from their actions are better able to determine for themselves when, how, and to what extent information about them is communicated to others. Although it does not offer seclusion in the usual spatial sense, being anonymous affords a kind of isolation. Whereas credit card payments create traceable transactions allowing a consumer's activities to be tracked and a data profile to be created, anonymous payments preserve privacy.

Historically, the value of anonymity had less to do with its privacy-enhancing potential than its political purpose. Anonymity has always been a crucial thread in the fabric of

democracy. Anonymous voting ensured that citizens were free actors, that their political participation would remain uninfluenced by the tyranny of the majority or by undue pressure from other powerful groups. The *Federalist Papers*, a bedrock of U.S. Constitutional thought, though not truly anonymous, were written pseudonymously using a fabricated name to cloak the identities of its authors while still allowing a mediated form of attribution. The same strategy was later employed by 19th century female novelists to prevent gender discrimination from influencing how their work was received.

Now, as then, anonymity enables people to discuss taboo subjects with others. Whether face-to-face in a self-help group or peer-to-peer in an online chat, sexual abuse, addiction and disease are regularly confronted and sometimes overcome anonymously. For many persons, the mere assurance of anonymity is what emboldens them to participate in the first place. Of course, anonymity also enables unlawful associations and anti-social behaviour, causing one U.S. Supreme Court Justice to refer to anonymity as the “refuge of scoundrels.”

In other legal systems, such as Canada’s, the ‘refuge’ that anonymity provides is seen as beneficial for the victims of crimes, imposing restrictions on the publication of their identities and in some cases requiring them to use pseudonyms. Although anonymity is imposed upon victims with good intentions, it is not always welcome, nor is it always a viable social solution.

Because anonymity can yield good or bad outcomes, some perceive a conflict regarding its value and role in democratic societies. In the United States, political anonymity is a constitutional entitlement flowing from the right to freedom of expression and freedom of association. But the right to anonymous communication is not immutable; it must be balanced against State interests in protecting people's reputations, fighting fraud and crime, and in safeguarding national security. Whereas few would disagree that anonymous voting is desirable and anonymous criminal activity is undesirable, between these extremes lies a sea of uncertainty. Should the internet support untraceable transactions? What is an appropriate national encryption policy?

As the internet continues to evolve, anonymity's future abounds with question marks. The information trade has turned dataveillance into big business. Cybercrime legislation and the expanding ability of law enforcement agencies to collect personal information and intercept electronic communications has been proposed or enacted in many jurisdictions, and the demands for identification for everything from air travel to building entry are on the rise. At the same time, blogs, chat rooms, instant messaging and a number of other online environments provide exciting new venues for social and political participation that permit and even encourage individuals to conceal their actual identities. Millions of people using them have made clear their desire to withhold disclosure of their identities for a variety of legitimate social purposes, inspiring a number of cryptographers to develop systems of provable anonymity. The extent to which such applications will be permitted or adopted by governments or markets in the 21st century remains uncertain. Their potential uses and broader questions concerning the importance and impact of

anonymity in a networked society are under investigation by a number of academics and privacy advocates.

Cross References

See also: Authentication; Identification; Internet Privacy;

Further Reading

Clarke, R. "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" [Online, December 2005] <<http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>>

Kerr, I R et al. *On the Identity Trail* <www.anonequity.org>

Marx, G.T. "What's in a Name? Some Reflections on the Sociology of Anonymity" *The Information Society* 15 (1999): 99-112.

Nissenbaum, H. "The Meaning of Anonymity in an Information Age" *The Information Society* 15 (1999): 141-144.

Ian R. Kerr

Ian R Kerr holds the Canada Research Chair in Ethics, Law and Technology at the University of Ottawa, Faculty of Law. He has published writings in academic books and journals on ethical and legal aspects of privacy, digital copyright, automated electronic commerce, artificial intelligence, cybercrime, nanotechnology, internet regulation, ISP liability, and online defamation. His current program of research includes *On the Identity Trail*, supported by one of the largest ever grants from the Social Sciences and Humanities Research Council, focusing on the impact of information and authentication technologies on our identity and our ability to be anonymous.