

## Ian Kerr: interview

Ian Kerr

Canada Research Chair in Ethics, Law & Technology &ndash; University of Ottawa  
Principal Investigator

e-mail: iankerr(at)uottawa.ca

ANON interviews Dr. Ian Kerr  
April, 2004

ANON: What challenges do you face as the principle investigator of an inter-disciplinary and multi-disciplinary collaborative initiative?

IAN KERR: The challenges arise administratively and substantively. The goal of this project, from an administrative point of view, is to get culturally distinct persons who are interested in the same sets of issues into the same room at the same time, speaking the same language, in order to help each other resolve common problems and achieve common goals. One challenge is that we are working with people who are so talented that they are constantly being called upon by various institutions and organizations. The other problem is that different disciplines sometimes speak different languages. This makes it more challenging to stay the course with common problems and goals but that is what we are trying to do. After all, there is no use in building a team if the individuals together do not create something better than what they can achieve as individuals. We are trying, as a team, to focus on resolving common problems in the privacy space in ways that are more useful and perhaps more valuable than if we were to do these things as individuals.

ANON: How did you choose the three research tracks for the anonymity project?

IAN KERR: I did not really choose the three tracks, they chose me. My research interests exist at the intersection between them. Lots of us on the team have a deep interest in the interdisciplinary aspects of this project. To the extent that I have influenced its interdisciplinarity, it is because I have always existed at the intersection between law & philosophy (specifically the philosophical questions raised by law and how law impacts philosophy). When information technology started to become popular in mid-90s, I began to realize that IT was a great setting to understand the fusion between law and philosophy. I teach a course in the graduate program called Technoprudence. In this course, we look at how new technologies actually change the way we philosophize and theorize about the law. As my interest in IT grew, I began to realize that there are broader implications of IT in the social sciences and humanities. In fact, there are all sorts of parallel inquires/debates that go on in these different disciplines without one knowing about the other. The parallel inquires can, at times, be counterproductive once two different groups meet. For example, if a philosopher says something using philosophical language that has a completely different meaning than how that concept is employed in the legal tradition. SSHRC has given us a chance to experiment; a chance to try to figure out ways to bridge that gap &ndash; to talk across the different disciplines.

ANON: What difficulties are apparent in trying to facilitate communication between NGOs, government, the private sector, social activists and academia? What are the advantages of engaging with these sectors?

IAN KERR: It is difficult when different cultures are speaking in different languages to different people. But as the Duke once put it in Shakespeare's 'As You Like It,' &ldquo;sweet are the uses of adversity which like the toad, ugly and venomous, wears yet a precious jewel in its head&rdquo;. By getting these different folks together, there are great possibilities for new synergies. We are striving to achieve such things in spite of differences in the way we communicate and the different interests we sometimes represent. When you bring together people who are interested in the same issues but have a different approach, you create a golden opportunity to get feedback that cuts across the cultural assumptions and theoretical presumptions, creating the prospect of discarding disciplinary biases. SSHRC has afforded

us this golden opportunity.

ANON: How does anonymity in an online environment compare with anonymity offline? Is the nature and value of anonymity different in each context?

IAN KERR: We are just starting to figure some of this out. When network technologies first came into the mainstream, I recall seeing a cartoon in *New Yorker Magazine*. It showed two dogs talking online while their master was out. The caption said something like, "The great thing about the internet is that no one knows that you are a dog." Just a few years later, another cartoon came out, alluding to the earlier one. This newer cartoon included the same two dogs, but then added another strip in which the computer replied to the dogs, indicating not only that it knew they were dogs but that it also knew that they had recently visited several websites, downloading pictures of Lassie. These cartoons cleverly represent a reality about shifting IT architectures and the fact that the way these things work is a matter of choice. IT can be built to preserve anonymity, or to track the identity and actions of people (and dogs!). We are trying to figure out more about what anonymity means because we see that the architectural choices are shifting. We are at a crucial point: do we want technology that allows a space for anonymity or will we create an IT space where the default is to identify each and every individual and her or transactions?

Though people have been working on these issues for quite some time now — for example, my colleague David Chaum has been writing about this stuff since the 1980s — we do not know everything that we need to about the different possible natures of online anonymity and, likewise, we do not know about the social values attached to the different approaches that could be adopted. A few years back, a Canadian company called ZeroKnowledge Systems was knee deep into this stuff, conducting some interesting research on anonymity. The purpose of one of these tools, Freedom, was to preserve some anonymity when people were browsing by segregating the different "nyms" (digital personas) that they expressed when surfing (eg, different personas for business, political or social reasons). You could use Freedom to surf with these different nyms in a way that would make it difficult for someone to link any of these online personas together. Though you do not hear much about the Freedom software these days, IT applications of this sort are important — especially in a world where, as the dogs have discovered, computers talk back! The ability for automated systems to collect, store and disseminate personal information that was gathered for one purpose, but used for another, has significantly increased, creating serious implications for safeguarding informational privacy. Some of the anonymizing technologies that my technology colleagues David Chaum, Stefan Brands and Steve Mann are experimenting with are exploring how different architectures can be employed to preserve some space for anonymous interaction and in some cases still allowing various forms of authentication to take place as is necessary for many institutions who truly cannot offer their services without collecting some information.

There are values for anonymous interactions, online and offline. And some of those values are very different from the typical picture that is being painted by certain power brokers. The media and the recording industries, for example, tend to paint a picture of online anonymity as though its only purpose is to extricate accountability. For example when college students use anonymity to hide-out while they upload and download music. Likewise, law enforcement often treats online anonymity as though its only social use is to commit cybercrime or acts of terrorism. Given these extreme characterizations of online anonymity and the tremendous impact that these are having on our chosen IT architectures, it is still too early to draw conclusions about the nature and value of online anonymity. Let us be clear though: despite it being early days, the fact that there is a value in preserving online anonymity is unquestionable. As is the case in other spaces, anonymous interaction can facilitate important discussions and other forms of social participation amongst groups in our society who, by virtue of various existing social norms, are otherwise unable to collect, express themselves or participate.

ANON: Do ISPs owe a fiduciary duty to users?

IAN KERR: We have data protection legislation in various parts of Canada that requires many of those who collect and store information, to treat it as though they are the trustees of that information. Fair Information Practices, as they are called, suggest that a company's need to collect, store and use people's personal information needs to be balanced against the privacy interests of the subjects of that information. The concept of a "fiduciary duty" — which entails that the person who owes the duty might sometimes be required to act in the interest of someone else regardless of his or her own self-interest may be held by the courts in the future to apply to an information intermediary, perhaps even an ISP. In some cases, what needs to be asked is whether the so-called "trustee" or information steward has an obligation to act in the interest of the information subject. If so, the information intermediary might have to refrain from disclosing information it might otherwise wish to disclose. To take a hot button example, ISPs in Canada have been under pressure by the Canadian Recording Industry Association (CRIA) to disclose personal information that would allow the recording industry to ascertain the identities of some of their subscribers. While the Federal Court of Canada did not explicitly say that a fiduciary obligation is owed by ISPs to users, it did consider the fact that the subscribers' privacy interests should be a factor, and that ISPs ought not to be compelled to disclose personal information about its subscribers unless certain thresholds are met. More and more, we are coming to see that ISPs and other information intermediaries are playing a role in safeguarding user and consumer privacy. And, to the extent that they do, the duties they might be said to owe to consumers to protect their identities is becoming increasingly significant consideration.

ANON: How important is it for ISPs to comply with their privacy policies?

IAN KERR: It is very important for ISPs to comply with their privacy policies. In failing to comply with these policies, an ISP could be in breach of contract and, in some cases, in breach of federal or provincial privacy data protection legislation. It could also be interfering with broader privacy interests that courts are sometimes willing to protect. A few years ago, Yahoo! acted in breach of its privacy policy when it revealed the identity of one of its users without notifying him (as promised in its privacy policy) . A lawsuit commenced. Although the case settled before going to court, the pressure of litigation, combined with the reaction of its customers worldwide taught Yahoo! that it is important to adhere to its privacy policy. There is a lesson in this for many online businesses who simply cut and paste privacy policies without giving much thought to them and without any clear plans to honour those policies.

ANON: What pressures do ISPs face in revealing the identity of their users?

IAN KERR: As part of one of the milestones attached to this project, we gave an industry workshop to Bell Canada in January because they, and other ISPs, are under pressure to reveal subscribers identities all the time. My portion of the workshop was titled the 'Unenviable position of ISPs'. Its aim was to offer ISPs a broader set of considerations to guide them in making difficult choices. The role of ISPs has been shifting. In the early days, the role of service providers was very much seen to include safeguarding a user's privacy. When the architectures became better understood, law enforcement agencies realized that the internet was a great source of investigatory information. Since the drafting of the European Convention on Cybercrime, there has been a lot of pressure on ISPs to reveal the identity of users. Part of this has to do with the lawful access agenda, as it is called, which tries to broaden the scope of information that can be lawfully accessed by law enforcement agencies in order to fight cybercrime and terrorism. ISPs are now stuck in the middle, one the one hand trying to preserve the privacy of users and, on the other hand, under pressure from private litigants and law enforcement officials.

ANON: Has the 'reasonable expectation of privacy' standard changed in the post-9/11 climate? Has attention to cybercrime altered this constitutional doctrine?

IAN KERR: Though less in Canada than in the US, I think that the standard has shifted and I am quite concerned about it. The reason why it is so important to maintain the a reasonable expectation of privacy is that, besides securing our right against unreasonable searches and other interferences with our basic liberties, it provides an important barometer for a well functioning democracy. The test of the strength of any democracy involves an indication of how it protects civil liberties when national security has been threatened. I believe our current political climate has been skewing the balance in favour of national security interests, sometimes at the unjustified expense of personal liberty. When public interest in national security becomes heightened, there is a tendency to look differently at the reasonable expectation of privacy standard.

Its not just how 9/11 has affected us. There is a word wide reaction to terrorism and cybercrime, some of which preceeded 9-11.. These global concerns are affecting our laws. Canada has signed but not yet ratified the European Convention on Cybercrime. There is a lot of pressure on the Canadian government to ratify this Convention. As signatories or parties to certain treaties, Canada is committed in a way that may have the ultimate affect of drafting laws that influence, and to some extent undermine, our reasonable expectation of privacy.

ANON: What are some of the legal and ethical implications of inverse surveillance? Is it potentially a powerful and effective form of civil disobedience?

IAN KERR: It may be a powerful and effective form of civil disobedience, but there are some risks in achieving inverse surveillance. In doing so, one runs the risk of breach privacy norms or failing to comply with fair information practices. Steve Mann and I will start looking at the question in a collaboration that begins in 2005.

ANON: How do automation technologies that protect digital copyright affect the right to privacy in Canada? What is the difference between a technical protection measure (TPM) and digital rights management (DRM) systems?

IAN KERR: We are not sure yet because there are no full fledged digital rights management systems currently in mainstream operation. The real question is whether those who build them will do so in a manner that complies with fair information practices. It may depend on who is building them and under what jurisdiction.

A technical protection measure (TPM) is a technology that operates as a virtual fence in order to protect copyrights by restricting access to or by controlling the use of a work subject to copyright. A DRM is a more elaborate system using TPMs and other technologies to manage the unbundling of copyright for owners and users. A DRM contains a database, which contains information about who holds rights and what rights are held by whom. It also contains information about which users have paid for what. DRMs use surveillance technologies to track and collect information about its users. By doing so, this technology enables people to license certain uses of the material in ways that they otherwise might not. It allows for creative modes of content delivery, but they come with a price. The only way that a DRM system can work is

through routine monitoring. Depending on its design, subscribers might not know that information about their habits and uses is being tracked, nor do they know who is using that information or what happens to it. The question up for grabs is whether mainstream DRM systems will be built to comply with privacy and fair information practices. We hope to convince industry partners like Bell Canada and IBM, and others working in and around this space, to influence the development of technologies that are privacy enhancing. There is nothing about the nature of these technologies that makes them unfriendly to privacy. Usually it comes down to who is building them and the ability of other power brokers to affect how these architectures will be constructed.

[Learn more about Ian Kerr](#)