THE STRANGE RETURN OF *GYGES' RING*: AN INTRODUCTION

Book II of Plato's *Republic* tells the story of a Lydian shepherd who stumbles upon the ancient Ring of Gyges while minding his flock. Fiddling with the ring one day, the shepherd discovers its magical power to render him invisible. As the story goes, the protagonist uses his newly found power to gain secret access to the castle where he ultimately kills the king and overthrows the kingdom.

Fundamentally, the ring provides the shepherd with an unusual opportunity to move through the halls of power without being tied to his public identity or his personal history. It also provided Plato with a narrative device to address a classic question known to philosophers as the "immoralist's challenge": why be moral if one can act otherwise with impunity?

THE NETWORK SOCIETY

In a network society—where key social structures and activities are organized around electronically processed information networks—this question ceases to be the luxury of an ancient philosopher's thought experiments. With the establishment of a global telecommunications network, the immoralist's challenge is no longer premised on mythology. The advent of the World Wide Web in the 1990s enabled everyone with access to a computer and modem to become unknown, and in some cases invisible, in public spaces—to communicate, emote, act, and interact with *relative* anonymity. Indeed, this may even have granted users more power than did Gyges' Ring, because the impact of what one could say or do online was no longer limited by physical proximity or corporeality. The end-to-end architecture of the Web's Transmission Control Protocol, for example, facilitated unidentified, one-to-many interactions at a distance. As the now-famous cartoon framed the popular culture of the early 1990s, "On the Internet, nobody knows you're a dog."[1] Although this cartoon resonated deeply on various levels, at the level of architecture it reflected the simple fact that the Internet's original protocols did not require people to identify themselves, enabling them to play with their identities—to represent themselves however they wished.

In those heady days bookmarking the end of the previous millennium, the rather strange and abrupt advent of Gyges' Ring 2.0 was by no means an unwelcome event. Network technologies fostered new social interactions of various sorts and provided unprecedented opportunities for individuals to share their

1. Peter Steiner, "On the Internet, Nobody Knows You're a Dog," *The New Yorker* (July 5, 1993), http://www.cartoonbank.com/item/22230.

thoughts and ideas en masse. Among other things, the Internet permitted robust political speech in hostile environments, allowing its users to say and do things that they might never have dared to say or do in places where their identity was more rigidly constrained by the relationships of power that bracket their experience of freedom. Anonymous browsers and messaging applications promoted frank discussion by employees in oppressive workplaces and created similar opportunities for others stifled by various forms of social stigma. Likewise, new cryptographic techniques promised to preserve personal privacy by empowering individuals to make careful and informed decisions about how, when, and with whom they would share their thoughts or their personal information.

At the same time, many of these new information technologies created opportunities to disrupt and resist the legal framework that protects persons and property. Succumbing to the immoralist's challenge, there were those who exploited the network to defraud, defame, and harass; to destroy property; to distribute harmful or illegal content; and to undermine national security.

In parallel with both of these developments, we have witnessed the proliferation of various security measures in the public and private sectors designed to undermine the "ID-free" protocols of the original network. New methods of authentication, verification, and surveillance have increasingly allowed persons and things to be digitally or biometrically identified, tagged, tracked, and monitored in real time and in formats that can be captured, archived, and retrieved indefinitely. More recently, given the increasing popularity of social network sites and the pervasiveness of interactive media used to cultivate user-generated content, the ability of governments, not to mention the proliferating international data brokerage industries that feed them, to collect, use, and disclose personal information about everyone on the network is increasing logarithmically. This phenomenon is further exacerbated by corporate and government imperatives to create and maintain large-scale information infrastructures to generate profit and increase efficiencies.

In this new world of ubiquitous handheld recording devices, personal webcams, interconnected closed circuit television (CCTV) cameras, radio frequency identification (RFID) tags, smart cards, global satellite positioning systems, HTTP cookies, digital rights management systems, biometric scanners, and DNA sequencers, the space for private, unidentified, or unauthenticated activity is rapidly shrinking. Many worry that the regulatory responses to the real and perceived threats posed by Gyges' Ring have already profoundly challenged our fundamental commitments to privacy, autonomy, equality, security of the person, free speech, free movement, and free association. Add in the shifting emphasis in recent years toward public safety and national security, and network technologies appear to be evolving in a manner that is transforming the structures of our communications systems from architectures of freedom to architectures of control. Are we shifting away from the original design of the network, from spaces where anonymity and privacy were once the default position to spaces where nearly every human transaction is subject to tracking, monitoring, and the possibility of authentication and identification?

The ability or inability to maintain privacy, construct our own identities, control the use of our identifiers, decide for ourselves what is known about us, and, in some cases, disconnect our actions from our identifiers will ultimately have profound implications for individual and group behavior. It will affect the extent to which people, corporations, and governments choose to engage in global electronic commerce, social media, and other important features of the network society. It will affect the way that we think of ourselves, the way we choose to express ourselves, the way that we make moral decisions, and our willingness and ability to fully participate in political processes. Yet our current philosophical, social, and political understandings of the impact and importance of privacy, identity, and anonymity in a network society are simplistic and poorly developed, as is our understanding of the broader social impact of emerging network technologies on existing legal, ethical, regulatory, and social structures.

This book investigates these issues from a number of North American and European perspectives. Our joint examination is structured around three core organizing themes: (1) privacy, (2) identity, and (3) anonymity.

PRIVACY

The jurist Hyman Gross once described privacy as a concept "infected with pernicious ambiguities."[2] More recently, Canadian Supreme Court Justice Ian Binnie expressed a related worry, opining that "privacy is protean."[3] The judge's metaphor is rather telling when one recalls that Proteus was a shape-shifter who would transform in order to avoid answering questions about the future. Perhaps U.S. novelist Jonathan Franzen had something similar in mind when he characterized privacy as the "Cheshire cat of values."[4]

One wonders whether privacy will suffer the same fate as Lewis Carroll's enigmatic feline—all smile and no cat.

Certainly, that is what Larry Ellison seems to think. Ellison is the CEO of Oracle Corporation and the fourteenth richest person alive. In the aftermath of September 11, 2001, Ellison offered to donate to the U.S. Government software that would enable a national identification database, boldly stating in 2004 that "The privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy."[5] As someone who understands the power of network databases to profile people right down to their skivvies

2. Hyman Gross, "The Concept of Privacy," *N.Y.U. L. Rev.* 43 (1967): 34–35.

3. *R. v Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, per Justice Binnie, at 25.

4. Jonathan Franzen, *How to Be Alone: Essays* (New York: Farrar, Straus and Giroux, 2003), 42.

5. Larry Ellison, quoted in L. Gordon Crovitz, "Privacy? We Got Over It" *The Wall Street Journal*, A11, August 25, 2008, http://online.wsj.com/article/SB121962391804567765.html?mod=rss_opinion_main.

(and not only to provide desirable recommendations for a better brand!), Ellison's view of the future of privacy is bleak. Indeed, many if not most contemporary discussions of privacy are about its erosion in the face of new and emerging technologies. Ellison was, in fact, merely reiterating a sentiment that had already been expressed some five years earlier by his counterpart at Sun Microsystems, Scott McNealy, who advised a group of journalists gathered to learn about Sun's data-sharing software: "You have zero privacy anyway. Get over it."[6]

To turn Hyman Gross's eloquent quotation on its head—the Ellison/McNealy conception of privacy is infected with ambiguous perniciousness. It disingenuously—or perhaps even malevolently—equivocates between two rather different notions of privacy in order to achieve a self-interested outcome: it starts with a *descriptive* account of privacy as the level of control an individual enjoys over her or his personal information and then draws a *prescriptive* conclusion that, because new technologies will undermine the possibility of personal control, we therefore ought *not* to expect any privacy.

Of course, the privacy that many of us expect is not contingent upon or conditioned by the existence or prevalence of any given technology. Privacy is a normative concept that reflects a deeply held set of values that predates and is not rendered irrelevant by the network society. To think otherwise is to commit what philosopher G. E. Moore called the "naturalistic fallacy,"[7] or as Lawrence Lessig has restyled it, the "is-ism":

> The mistake of confusing how something is with how it must be. There is certainly a way that cyberspace *is*. But how cyberspace *is* is not how cyberspace has to be. There is no single way that the net has to be; no single architecture that defines the nature of the net. The possible architectures of something that we would call "the net" are many, and the character of life within those different architectures are [sic] diverse.[8]

Although the "character of life" of privacy has, without question, become more diverse in light of technologies of both the privacy-diminishing and privacy-preserving variety, the approach adopted in this book is to understand privacy as a *normative* concept. In this approach, the existence of privacy rights will not simply depend on whether our current technological infrastructure has reshaped our privacy expectations in the descriptive sense. It is not a like-it-or-lump-it proposition. At the same time, it is recognized that the meaning, importance, impact, and implementation of privacy may need to evolve alongside the emergence of new technologies. How privacy ought to be understood—and fostered—in

6. *Ibid.*, Scott McNealy quote.

7. G. E. Moore, *Principia Ethica* (Cambridge: Cambridge University Press, 1903).

8. Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006): 32.

a network society certainly requires an appreciation of and reaction to new and emerging network technologies and their role in society.

Given that the currency of the network society is information, it is not totally surprising that privacy rights have more recently been recharacterized by courts as a kind of "informational self-determination."[9] Drawing on Alan Westin's classic definition of informational privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others,"[10] many jurisdictions have adopted fair information practice principles[11] as the basis for data protection regimes.[12] These principles and the laws that support them are not a panacea, as they have been developed and implemented on the basis of an unhappy compromise between those who view privacy as a fundamental human right and those who view it as an economic right.[13] From one perspective, these laws aim to protect privacy, autonomy, and dignity interests. From another, they are the lowest common denominator of fairness in the information trade. Among other things, it is thought that fair information practice principles have the potential to be technology neutral, meaning that they apply to any and all technologies so that privacy laws do not have to be rewritten each time a new privacy-implicating technology comes along. A number of chapters in this book challenge that view.

Our examination of privacy in Part I of this book begins with the very fulcrum of the fair information practice principles—the doctrine of consent. Consent is often seen as the legal proxy for autonomous choice and is therefore anchored in the traditional paradigm of the classical liberal individual, which is typically thought to provide privacy's safest harbor. As an act of ongoing agency, consent can also function as a gatekeeper for the collection, use, and disclosure of personal information. As several of our chapters demonstrate, however, consent can also be manipulated, and reliance on it can generate unintended consequences in and outside of privacy law. Consequently, we devote several chapters

9. Known in German as "Informationelles selbstbestimmung," this expression was first used jurisprudentially in Volkszählungsurteil vom 15. Dezember 1983, BVerfGE 65, 1, German Constitutional Court (Bundesverfassungsgerichts) 1983.

10. Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967): 7.

11. Organization for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* Annex to the Recommendation of the Council of 23 September 1980, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

12. Article 29 of Directive EC, Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] O.J. L. 281: 31; Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

13. Canada. House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities. 35th Parliament, 2nd Session. *Privacy: Where Do We Draw the Line?* (Ottawa: Public Works and Government Services Canada, 1997).

to interrogations of the extent to which the control/consent model is a sufficient safeguard for privacy in a network society.

Does privacy live on liberal individualism alone? Some of our chapters seek out ways of illuminating privacy in light of other cherished collective values such as equality and security. Although the usual temptation is to understand these values as being in conflict with privacy, our approach in this book casts privacy as complementary to and in some cases symbiotic with these other important social values. Privacy does not stand alone. It is nested in a number of social relationships and is itself related to other important concepts, such as identity and anonymity. We turn to those concepts in Parts II and III of the book.

IDENTITY

Although lofty judicial conceptions of privacy such as "informational self-determination" set important normative standards, the traditional notion of a pure, disembodied, and atomistic self, capable of making perfectly rational and isolated choices in order to assert complete control over personal information, is not a particularly helpful fiction in a network society. If a fiction there must be, one that is perhaps more worthy of consideration is the idea of identity as a theft of the self. Who we are in the world and how we are identified is, at best, a concession. Aspects of our identities are chosen, others assigned, and still others accidentally accrued. Sometimes they are concealed at our discretion, other times they are revealed against our will. Identity formation and disclosure are both complex social negotiations, and in the context of the network society, it is not usually the individual who holds the bargaining power.

Because the network society is to a large extent premised on mediated interaction, who we are (and who we say we are) is not a self-authenticating proposition in the same way that it might be if we were close kin or even if we were merely standing in physical proximity to one another. Although we can be relatively certain that it is *not* a canine on the other end of an IM chat, the identity of the entity at the other end of a transaction may be entirely ambiguous. Is it a business partner, an imposter, or an automated software bot?

The same could be true of someone seeking to cross an international border, order an expensive product online, or fly an airplane—assuming she or he is able to spoof the appropriate credentials or identifiers. As we saw in the extreme example of the shepherd in possession of Gyges' Ring, those who are able to obfuscate their identities sometimes take the opportunity to act with limited accountability. This is one of the reasons why network architects and social policymakers have become quite concerned with issues of identity and identification.

However, it is important to recognize that identification techniques can preserve or diminish privacy. Their basic function is to make at least some aspects of an unknown entity known by mapping it to a knowable attribute.

An identification technique is more likely to be privacy preserving if it takes a minimalist approach with respect to those attributes that are to become known. For example, an automated highway toll system may need to authenticate certain attributes associated with a car or driver in order to appropriately debit an account for the cost of the toll. But to do so, it need not identify the car, the driver, the passengers, or for that matter the ultimate destination of the vehicle. Instead, anonymous digital credentials[14] could be assigned that would allow cryptographic tokens to be exchanged through a network in order to prove statements about them and their relationships with the relevant organization(s) without any need to identify the drivers or passengers themselves. Electronic voting systems can do the same thing.

In Part II of the book we explore these issues by investigating different philosophical notions of identity and discussing how those differences matter. We also address the role of identity and identification in achieving personal and public safety. We consider whether a focus on the protection of "heroic" cowboys who refuse to reveal their identities in defiance of orders to do so by law enforcement officers risks more harm than good, and whether unilateral decisions by the State to mandate control over the identities of heroic sexually assaulted women as a protective measure risk less good than harm. We examine the interaction of self and other in the construction of identity and demonstrate in several chapters why discussions of privacy and identity cannot easily be disentangled from broader discussions about power, gender, difference, and discrimination.

We also examine the ways in which identity formation and identification can be enabled or disabled by various technologies. A number of technologies that we discuss—data-mining, automation, ID cards, ubiquitous computing, biometrics, and human-implantable RFID—have potential narrowing effects, reducing who we are to how we can be counted, kept track of, or marketed to. Other technologies under investigation in this book—mix networks and data obfuscation technologies—can be tools for social resistance used to undermine identification and the collection of personal information, returning us to where our story began.

ANONYMITY

We end in Part III with a comparative investigation of the law's response to the renaissance of anonymity. Riffing on Andy Warhol's best known turn of phrase, an internationally (un)known British street artist living under the pseudonym "Banksy"[15] produced an installation with words on a retro-looking pink screen

14. David Chaum, "Achieving Electronic Privacy," *Scientific America* (August 1992): 96–101; Stefan A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy* (Cambridge, MA: MIT Press, 2000).

15. Banksy, "By Banksy," http://www.banksy.co.uk/- (accessed September 10, 2008).

that say, "In the future, everyone will have their 15 minutes of anonymity."[16] Was this a comment on the erosion of privacy in light of future technology? Or was it a reflection of Banksy's own experience regarding the challenges of living life under a pseudonym in a network society? Whereas Warhol's "15 minutes of fame" recognized the fleeting nature of celebrity and public attention, Banksy's "15 minutes of anonymity" recognizes the long-lasting nature of information ubiquity and data retention.

Although privacy and anonymity are related concepts, it is important to realize that they are not the same thing. There are those who think that anonymity is the key to privacy. The intuition is that a privacy breach cannot occur unless the information collected, used, or disclosed about an individual is associated with that individual's identity. Many anonymizing technologies exploit this notion, allowing people to control their personal information by obfuscating their identities. Interestingly, the same basic thinking underlies most data protection regimes, which one way or another link privacy protection to an identifiable individual. According to this approach, it does not matter if we collect, use, or disclose information, attributes, or events about people so long as the information cannot be (easily) associated with them.

Although anonymity, in some cases, enables privacy, it certainly does not guarantee it. As Bruce Schneier has pointed out[17] and as any recovering alcoholic knows all too well, even if Alcoholics Anonymous does not require you to show ID or to use your real name, the meetings are anything but private. Anonymity in public is quite difficult to achieve. The fact that perceived anonymity in public became more easily achieved through the end-to-end architecture of the Net is part of what has made the Internet such a big deal, creating a renaissance in anonymity studies not to mention new markets for the emerging field of identity management. The AA example illustrates another crucial point about anonymity. Although there is a relationship between anonymity and invisibility, they are not the same thing. Though Gyges' Ring unhinged the link between the shepherd's identity and his actions, the magic of the ring[18] was not merely in enabling him to act anonymously (and therefore without accountability): the real magic was his ability to act invisibly. As some leading academics have recently come to

16. Banksy, interviewed by Shepard Fairey in "Banksy," *Swindle Magazine*, no. 8 (2008), http://swindlemagazine.com/issue08/banksy/ (accessed September 10, 2008).

17. Bruce Schneier, "Lesson From Tor Hack: Anonymity and Privacy Aren't the Same," *Wired* (September 20, 2007), http://www.wired.com/politics/security/commentary/securitymatters/2007/09/security_matters_0920?currentPage=2 (accessed September 10, 2008).

18. Arthur C. Clarke's famous third law states, "Any sufficiently advanced technology is indistinguishable from magic." See Arthur C. Clarke, http://www.quotationspage.com/quotes/Arthur_C._Clarke/, *Profiles of the Future; An Inquiry Into the Limits of the Possible* (Toronto: Bantam Books, 1971).

realize, visibility and exposure are also important elements in any discussion of privacy, identity, and anonymity.[19] Indeed, many argue that the power of the Internet lies not in the ability to hide who we are, but in freeing some of us to expose ourselves and to make ourselves visible on our own terms.

Given its potential ability to enhance privacy on one hand and to reduce accountability on the other, what is the proper scope of anonymity in a network society?

Although Part III of the book does not seek to answer this question directly, it does aim to erect signposts for developing appropriate policies by offering a comparative investigation of anonymity and the law in five European and North American jurisdictions. How the law regards anonymity, it turns out, is not a question reducible to discrete areas of practice. As we shall see, it is as broad ranging as the law itself.

Interestingly, despite significant differences in the five legal systems and their underlying values and attitudes regarding privacy and identity, there seems to be a substantial overlap in the way that these legal systems regard anonymity, which is not generally regarded as a right and certainly not as a foundational right. In the context of these five countries, it might even be said that the law's regard for anonymity is to some extent diminishing.

When one considers these emerging legal trends alongside the shifting technological landscape, it appears that the answer to our question posed at the outset is clear: the architecture of the network society seems to be shifting from one in which anonymity was the default to one where nearly every human transaction is subject to monitoring and the possibility of identity authentication. But what of the strange return of Gyges' Ring and the network society in which it reemerged? And what do we wish for the future of privacy, identity, and anonymity?

Let us begin the investigation.

19. Hille Koskela, "'In Visible City': Insecurity, Gender, and Power Relations in Urban Space," in *Voices from the North. New Trends in Nordic Human Geography*, eds. J. Öhman and K. Simonsen (Burlington: Ashgate, Aldershot, 2003): 283–294; Julie Cohen, "Privacy, Visibility, Transparency, and Exposure," *University of Chicago Law Review* 75, no. 1 (2008); Kevin D. Haggerty and Richard V. Ericson, *The New Politics of Surveillance and Visibility* (Toronto: University of Toronto Press, 2005).