CHAPTER NINE

Digital Locks and the Automation of Virtue

Ian Kerr*

"And what is good, Phaedrus,
And what is not good —
Need we ask anyone to tell us these things?"[1]

A. INTRODUCTION

Of all the "lock and key" narratives in the western cannon,[2] I think my favorite is the legend of the Gordian knot. Midas, the son of King Gordius,

---

* This chapter derives from two keynote addresses delivered in 2006 at New York University and the Banff Centre. I would like to thank Helen Nissenbaum, Michael Zimmer and Greg Hagen for those very special invitations. Thanks also to Niva Elkin-Koren and Abraham Drassinower for sharing their memorable insights following those lectures and to Dan Hunter, old bean, for making me promise to one day put the NYU keynote into writing (yes, I am slow to deliver). My work has — then and now — enjoyed tremendous support from the Social Sciences and Humanities Research Council and the Canada Research Chairs program and I am grateful for their generous contributions. Thanks also to jennifer barrigar, Michael Geist, David Matheson, Jason Millar, and the anonymous peer reviewers for their invaluable comments on an earlier draft. Special thanks to Golsa Ghamari, Sinziana Gutiu, and Kristen Thomasen for their brilliance, and for the high quality of research assistance that they so regularly and reliably provide. Saving the best for last, my extreme gratitude goes out on this one to Katie Szilagyi — engineer, law student *par excellence* and proud owner of these fine footnotes — for grace under pressure, her tireless enthusiasm, her ability to find anything under the sun, her insatiable intellectual curiosity, and her deep-seated disposition for *arête* . . . which she has not only cultivated for herself but, through collaboration, inspires in others.

1 Robert Pirsig, *Zen and the Art of Motorcycle Maintenance: An Inquiry into Values* (New York: Bantam, 1974) (epigraph).

2 For example, in the tale of Ali Baba and the Forty Thieves, the treasure chamber remained locked and inaccessible until the key — in this case the code words "Open

intricately tied the famous knot. It was initially fabricated as a physical lock. Woven in unfathomable complexity, the knot fastened his father's famous ox-cart[3] to a wooden post. As the Greek historian Plutarch described it, Midas tethered the ox-cart, "fastened to its yoke by the bark of the cornel-tree . . . the fastenings so elaborately intertwined and coiled upon one another that their ends were hidden."[4] Secured by the knot, Midas intended the cart to remain locked within the palace compound of the former kings of Phrygia at Gordium as an enduring legacy of his family's rule. However, due to a prophecy of the oracle of Telmissus, the knot became known not so much for what it prevented as for what it would one day permit. Indeed, the multitudes that sought to disentangle it over the years never intended to steal the cart. Rather, they hoped to fulfill the oracle's prophecy that, "was believed by all the barbarians, that the fates that decreed that the man who untied the knot was destined to become ruler of the whole world."[5]

Perhaps because of this rather strange divination, the Gordian knot became known in the region as a seemingly intractable puzzle, an intel-

---

Sesame!" — was uttered aloud. See Katie Daynes and Paddy Mounter, *Ali Baba and The Forty Thieves* (London: Usborne Publishing, 2007). In a famed fairy tale, heroine Rapunzel is locked in her tower with no way of entry, mandated to release her long hair as the golden stair/access key whenever the evil enchantress demands. When the enchantress discovers Rapunzel has been allowing a male suitor to also climb upon her hair, it is cut off — removing the key to the tower. Jacob Grimm, Wilhelm Grimm & Dorothée Duntze, *Rapunzel*, trans by. Anthea Bell (New York: North-South Books, 2007). The Lion, The Witch and the Wardrobe, one of C.S. Lewis' most famous stories from "The Chronicles of Narnia" series, uses a wardrobe as the gateway to the magical land of Narnia. The children are transported to Narnia, forgetting their real home in the process. They remain locked in Narnia until a lamppost triggers their memories. Their memories are the key to unlocking the wardrobe, enabling them to arrive back home. See C.S. Lewis, *The Lion, The Witch and The Wardrobe* (London: Geoffrey Bles, 1950).

3 Midas and his father, Gordius, appeared in town on the fabled ox-cart at a particularly auspicious time. An oracle had foretold that the new king would be brought to the Phrygians upon an ordinary ox-cart and that the appearance of an eagle would signify future greatness. Gordius was proclaimed king, ending the civil war in the region, and beginning the Phrygian dynasty. See Graham Anderson, *Folktale as a Source of Graeco-Roman Fiction: The Origin of Popular Narrative* (Lewiston, NY: Edwin Meller Press, 2007) at 53. For the significance of the Gordian knot, see Lynn E. Roller, "Midas and the Gordian Knot" (1984) 3:2 Classical Antiquity at 256–71. For discussion of the legend of Midas more generally, see Lynn E. Roller, "The Legend of Midas" (1983) 2:2 Classical Antiquity at 299–313.

4 Plutarch, *The Age of Alexander: Nine Greek Lives By Plutarch*, trans. by Ian Scott-Kilvert (Harmondsworth: Penguin Books, 1973) at 271.

5 *Ibid.*

lectual lock requiring an intellectual key. According to the legend, numerous puzzlers visited the palace with the hope of unlocking the mystery of the knot and winning the kingdom. Many tried and failed over the years. Finally, in one version of the legend, Alexander the Great discovered a solution during his visit to the palace; he swiftly drew his sword, slicing through the knot rather than untying it by hand.

For the most part, history has declared Alexander the hero of the prophecy. His defiant, brute force solution of hacking the knot with his sword has become a metaphor not only for resolving difficult problems by unanticipated means, but "with a single dramatic stroke."[6] Having abstracted the problem as one of freeing the ox-cart from the post rather seeing it merely as a problem of manually untying the knotted cord, the Alexandrian solution is a quintessential example of the gestalt shift,[7] and of the idea that true problem solving often requires violating established conventions. The Alexandrian solution also reminds us that anything that can be built can be un-built, anything that can be locked, unlocked.

This chapter is about digital locks. Like the Gordian knot, digital locks are, in part, designed as a restraint on the use of property. Only, these newer technical protection measures (TPMs) employ cryptographic rather than physical entanglements with the aim of precluding people from using digital works in ways that the copyright owner does not wish. Digital locks can be wrapped around music, movies, books, newspapers and other digital content to prevent or limit access to those works, or to control the number of copies made. They can also be woven into the code of electronic devices such as computers, e-book readers, phones and other media players to restrict customers from using competitors' applications and products. Like the Gordian knot, digital locks can be hacked. And, not unlike the

---

6 W. Russell Neuman, Lee McKnight, & Richard Jay Solomon, *The Gordian Knot: Political Gridlock on the Information Highway* (Cambridge: The MIT Press, 1997) at ix.

7 The gestalt shift refers to an abrupt, involuntary shift in perception that enables an observer to see something in a different manner. The object of the shift is unaltered; the only change is in the viewer's perception of the object. The German word "gestalt" means "shape" or "form" in English. The sudden refocusing is said to take place suddenly and *in toto*. Celebrated examples include an image of a duck that can also be seen as a rabbit or an image of two women in profile facing one another that can also represent a vase. The shift from one to another takes place instantaneously and encompasses the totality of the image — it is not a matter of degrees. See Robert Wade, "Gestalt Shift: From 'Miracle' to 'Cronyism' in the Asian Crisis" (February 2002), London School of Economics and Political Science Development Studies Institute, www2.lse.ac.uk/internationalDevelopment/pdf/WP25.pdf. See also Robert Angelo, "Gestalt Shift," www.roangelo.net/logwitt/gestalt-shift.html.

oracle of Telmissus, some digital lock-makers have even tendered challenges to would-be hackers to try to crack their codes, proffering rewards in exchange for details about how the lock might be defeated.[8] Recognizing that all locks can be broken, many of those who employ digital locks have sought the further protection of law, lobbying lawmakers to make it illegal to circumvent digital locks.[9]

---

8 The Secure Digital Music Initiative (SDMI) was a project designed to prevent digital music sharing through the implementation of anti-piracy measures such as watermarking. To assist in the creation of a robust security system and aid in identifying possible holes in four potential technologies, SDMI issued a public challenge to researchers in the field. Over the course of three weeks in September 2000, researchers were invited to download the watermarked music files and attempt to remove the watermarks. A team of researchers from Princeton and Rice Universities, headed by computer scientist and security expert Edward Felten, successfully met the challenge, removing all four different watermarks without degrading the quality of the music files. They opted against signing a confidentiality agreement that would have made them eligible for the cash prize. Instead, the team wrote a paper detailing their findings, which they planned to present at a 2001 conference. The Recording Industry Association of America (RIAA) and SDMI threatened legal action under the *Digital Millennium Copyright Act* for circumventing an owner's copyright protections (despite having been previously invited to do exactly that), if the findings were made publicly available. Felten chose not to publish under this threat, instead initiating his own lawsuit against SDMI under freedom of expression. The lawsuit was later dismissed by the United States District Court of New Jersey for lack of standing, but it remains a key example to highlight differences in security policies. Felten's paper was not intended to be a "how-to" guide for the layperson, using technical language that would have been unintelligible to everyone but those who intimately understood the technology. From a full disclosure perspective, disclosing the weaknesses of a security system will aid its creators in identifying any loopholes and strengthening protection measures as quickly as possible. In contrast, a security from obscurity viewpoint, seemingly preferred by the RIAA and SDMI in this case, would favour keeping information about system weaknesses secret, hoping that no one will identify them. Felten commented on this issue in particular, stating that the weaknesses in the technology were clear and that interested parties would overcome them, regardless of whether or not his paper was published. See Electronic Frontier Foundation, "*Felten, et. al. v. RIAA, et. al.*" http://w2.eff.org/IP/DMCA/Felten_v_RIAA. See also Electronic Frontier Foundation, "Final Hearing Transcript, *Felten v. RIAA* (Nov. 28, 2001)" http://w2.eff.org/IP/DMCA/Felten_v_RIAA/20011128_hearing_transcript.html. See also Scarlet Pruitt, "Silenced Professor Sues SDMI, RIAA" *PCWorld* (6 June 2001), www.pcworld.com/article/52006/silenced_professor_sues_sdmi_riaa.html.

9 This letter from the US Motion Picture and Television Industry and Labour Organizations to USTR Ambassador Ron Kirk regarding ACTA Negotiations showcases the vested interests of entertainment industries in robust legislative copyright protections. Letter from Motion Picture Association of America *et al.* to Ambassasor Ron Kirk (22 September 2009), www.mpaa.org/resources/ace3793e-cfaf-4749-96ae-385f38506268.pdf.

In this chapter, I investigate various potential uses of digital locks and the social consequences of creating laws that would make it illegal to circumvent them. I suggest that laws protecting an unimpeded use of digital locks — such as the one recently tabled in Canada[10] — are Gordian in the sense of the oracle's prophecy. That is, these laws will ultimately cause digital locks to become better known for what they permit than for what they preclude. This, I claim, is because digital locks are the key technology underlying a relatively new and extremely powerful form of social control: *the automation of permissions*.[11]

While the policy debate about digital locks has to date focused almost exclusively on their narrow role in copyright reform,[12] I will argue that

---

In the Canadian context, while a new Conservative cabinet was being sworn in on 6 February 2006, a lobbyist for the Canadian Recording Industry Association named David Dyer emailed the Director General of Canadian Heritage's Copyright Policy Branch recommending organizing an event about copyright reform. See Michael Geist, "CRIA's Lobby Effort: The Untold Story" (11 June 2006), www.michaelgeist.ca/index.php?option=com_content&task=view&id=1293.

10 Bill C-32 is the third bill designed to amend Canada's *Copyright Act* in recent years. Its predecessors, Bill C-60 and Bill C-61, both died on the order paper due to dissolution of Parliament. Bill C-32, *An Act to amend the Copyright Act*, 3d Sess., 40th Parl., 2010, www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4580265&file=4 [Bill C-32]. Bill C-61, *An Act to amend the Copyright Act*, 2d Sess., 39th Parl., 2008, www2.parl.gc.ca/HousePublications/redirector.aspx?RefererUrl=Publication.aspx%3fDocid=3570473%26file%3d4. Bill C-60, *An Act to amend the Copyright Act*, 1st Sess., 38th Parl., 2005, www2.parl.gc.ca/HousePublications/redirector.aspx?RefererUrl=Publication.aspx%3fDocid=2334015%26file%3d4.

11 Though not labeled as such, what I am calling the "automation of permissions" is a key strategy in the development of what Professor Lawrence Lessig refers to as a "permission culture"; see Lawrence Lessig, *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (New York: The Penguin Press, 2004), www.free-culture.cc/freecontent at xiv, 8, 173, 192–93. I will elaborate on both of these concepts below.

12 Andrew A. Adams & Ian Brown, "Keep Looking: The Answer to the Machine is Elsewhere" (2009) 19 Computers & L. 32 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1329703; Nika Aldrich, "A System of Logo-Based Disclosure of DRM on Download Products" (29 April, 2007), www.ssrn.com/abstract=983551; Stefan Bechtold, "Digital Rights Management in the United States and Europe" (2004) 52 Am. J. Comp. L. 323, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=732825; Dan L. Burk & Tarleton L. Gillespie, "Autonomy and Morality in DRM and Anti-Circumvention Law" (2006) 4 Triple C: Cognition, Communication, Cooperation 239, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1146448; Lee A. Bygrave, "Digital Rights Management and Privacy — Legal Aspects in the European Union" in Eberhard Beckar *et al.*, eds. *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (New York: Springer, 2003) 418, http://folk.uio.no/lee/publications/DRM_privacy.pdf; Julie E. Cohen, "DRM & Privacy" (2003) 18

digital locks are of even greater social significance when properly understood in light of their role in larger digital rights management (DRM) systems that are employed well beyond the copyright context. I will argue that the broader automation of permissions through DRM is the enabler

---

Berkeley L. & Tech J. 575, www.law.berkeley.edu/journals/btlj/articles/vol18/Cohen.stripped.pdf; Carys J. Craig, "Digital Locks and the Fate of Fair Dealing in Canada: In Pursuit of "Prescriptive Parallelism" (2010) 13 J. World Intellectual Property 503, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1599610; Jeremy F. DeBeer, "Locks & Levies" (2006) 84 Denv U.L. Rev. 143, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952128 ; Peter Drahos, *A Philosophy of Intellectual Property* (Sudbury MA: Dartmouth Publishing Group, 1996), http://epublications.bond.edu.au/blr/vol8/iss2/7/; Edward Felten, "A Skeptical View of DRM and Fair Use" (2003) 46 Communications of the ACM 4 at 57–59, http://cacm.acm.org/magazines/2003/4/6849-a-skeptical-view-of-drm-and-fair-use/fulltext; Daniel J. Gervais, "The Purpose of Copyright Law in Canada" (2006) 2 UOLTJ 2 at 315, http://works.bepress.com/daniel_gervais/10; Kamiel J. Koelman, "The Levitation of Copyright: An Economic View of Digital Home Copying, Levies and DRM" (2005) 4 Ent. L. Rev. 75, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=682163; Niva Elkin-Koren, "Making Room for Consumers Under the DMCA" (2007) 22 Berkeley Tech. L.J. 1119, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1024566; Michael Geist, "Anti-Circumvention Legislation and Competition Policy: Defining a Canadian Way?" in Michael Geist, ed., *In The Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005) 211, www.irwinlaw.com/pages/content-commons/anti-circumvention-legislation-and-competition-policy--defining-a-canadian-way----michael-geist; Tarleton L. Gillespie, "Designed to 'Effectively Frustrate': Copyright, Technology, and the Agency of Users" (2006) 8 New Media & Society 651, http://nms.sagepub.com/content/8/4/651.abstract; Graham Greenleaf, "Unlocking IP to Stimulate Australian Innovation: An Issues Paper" (2008) 44 University of New South Wales Faculty of Law Research Series, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1398604; Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006), http://codev2.cc/; Mark Perry, "Rights Management Information" in Michael Geist, ed., *In The Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005) 251, www.irwinlaw.com/pages/content-commons/rights-management-information---mark-perry; Matthew Rimmer, *Digital Copyright and the Consumer Revolution: Hands off my iPod* (Cheltenham: Edward Elgar Publishing, 2007), http://works.bepress.com/matthew_rimmer/1; Pamela Samuelson & Jason Schultz, "Regulating Digital Rights Management Technologies: Should Copyright Owners Have to Give Notice About DRM Restrictions?" (2007) J. Telecomm. & High Tech. L. http://people.ischool.berkeley.edu/~pam/papers/notice%20of%20DRM-701.pdf; Pamela Samuelson, "Digital Rights Management {and, or, vs.} the Law" (2003) 46 Communications of the AC 4, http://portal.acm.org/citation.cfm?id=641205.641229 at 41; Kimberlee G. Weatherall, "On Technology Locks and the Proper Scope of Digital Copyright Laws — Sony in the High Court" (2004) 26 Sydney L. Rev. 613 http://works.bepress.com/kimweatherall/2; Peter K. Yu, "Anticircumvention and Anti-anticircumvention" (2006) 84 Denv. U.L. Rev. 13 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=931899.

and catalyst of a potentially debilitating world, in which technology can be used to shift social defaults from inclusion to exclusion by disabling human action across a wide range of activities for all those who do not have prior permission from those controlling the DRM. While a well-established body of literature has very thoughtfully and carefully investigated the risks that excessive legal protection of digital locks can pose to access to information,[13] freedom of expression,[14] privacy,[15] encryption research,[16]

---

13 Bernt Hugenholtz, "Copyright, Contract and Code: What Will Remain of the Public Domain," (2000) 26 Brook. J. Int'l L. 77; Michael Geist, "Canada Rejects One-Sided Approach to Copyright Reform" *The Toronto Star* (28 March 2005), www.michaelgeist.ca/resc/html_bkup/mar282005.html.

14 Ian R. Kerr & Jane Bailey, "The Implications of Digital Rights Management for Privacy and Freedom of Expression" (2004) 2 Info. Comm. & Ethics in Society 87; Mark Perry and Casey Chisick, "Copyright and Anti-circumvention: Growing Pains in a Digital Millennium," (2000) New Zealand Int. Prop. J. 261, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1622851; Kamiel J. Koelman, "The protection of technological measures vs. the copyright limitations," ALAI Congress 2001, www.ivir.nl/publications/koelman/alaiNY.html; David Nimmer, "A Riff on Fair Use in the *Digital Millennium Copyright Act*," (2000) 148 U. Pa.L.Rev. 673.

15 Julie E. Cohen, "DRM & Privacy" (2003) 18 Berkeley L. & Tech J. 575, www.law.berkeley.edu/journals/btlj/articles/vol18/Cohen.stripped.pdf; Lee A. Bygrave, "The Technologisation of Copyright: Implications for Privacy and Related Interests" (2002) 24 European Intellectual Property Review 2 at 51; Ian Goldberg, "Privacy-enhancing technologies for the Internet, II: Five Years Later" (2002) Workshop on Privacy Enhancing Technologies, www.cypherpunks.ca/~iang/pubs/pet2.pdf at 1–2; Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004).

16 See *Amicus Curiae* Brief in Support of Appellants, *Universal v. Reimerdes* (26 Jan 2001), www.2600.com/dvd/docs/2001/0126-crypto-amicus.txt. ("The *amici curiae* are cryptographers, individuals whose work or hobby involves research, design, analysis, and testing of encryption technologies. *Amici* are concerned that Section 1201 of the *Digital Millennium Copyright Act* ("DMCA"), as construed by the District Court . . . would deprive cryptographers of the most effective language in which to communicate their research and its results, with the effect of weakening security systems and technological protection of data for the public."); Severine Dusollier, "Electrifying the Fence: The Legal Protection of Technological Protection Measures for Protecting Copyright" (1999) 21 Eur. Int. Prop. R. 285, www.crid.be/pdf/public/4138.pdf; Yochai Benkler, "Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain" (1999) 74 N.Y.U. L. Rev. 354 at 419; Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006), http://codev2.cc/; Edward Felten *et al.*, "Lest We Remember: Cold-Boot Attacks on Encryption Keys" (2009) 52 Communications of the ACM 5 at 91, http://citp.princeton.edu/pub/coldboot.pdf.

freedom to tinker,[17] education,[18] and copyright's delicate balance between owner and user rights,[19] my aim in this chapter is to make a more fundamental — perhaps foundational — claim.

I argue that a generalized and unimpeded use of digital locks, further protected by the force of law, threatens not merely the above enumerated legal rights and freedoms but also threatens to significantly impair our moral development. In particular, I express deep concern that digital locks

---

17 According to Ed Felten, the freedom to tinker "is your freedom to understand, discuss, repair and modify the technological devices you own." See Ed Felten, "My Experiment with 'Digital Drugs'" *Ed Felten's Blog*, www.freedom-to-tinker.com/blog/felten.

18 Samuel E. Trosow, "The Changing Landscape of Academic Libraries and Copyright Policy: Interlibrary Loans, Electronic Reserves, and Distance Education," in Michael Geist, ed., *In The Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005) 375, www.irwinlaw.com/pages/content-commons/the-changing-landscape-of-academic-libraries-and-copyright-policy--interlibrary-loans-electronic-reserves-and-distance-learning---samuel-trosow; C. Risher, "Technological protection measures (anti-circumvention devices) and their relation to exceptions to copyright in the Electronic environment" (Paper presented to the IPA Copyright Forum Frankfurt Book Fair, 20 October 2000) [unpublished]; Neil Postman, *The End of Education: Redefining the Value of School* (New York: Alfred A. Knopf, 1996) at 192; Dan L. Burk & Julie E. Cohen, "Fair Use Infrastructure for Copyright Management Systems" (2001) 15 Harv. J.L. & Tech. 41 at 63, www.law.georgetown.edu/Faculty/jec/fairuseinfra.pdf.

19 Abraham Drassinower, "Taking User Rights Seriously" in Michael Geist, ed., *In The Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005) 479, www.irwinlaw.com/pages/content-commons/taking-user-rights-seriously---abraham-drassinower; Jane Bailey, "Deflating the Michelin Man: Protecting Users' Rights in the Canadian Copyright Reform Process" in Michael Geist, ed., *In The Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005) 125, www.irwinlaw.com/pages/content-commons/deflating-the-michelin-man--protecting-users-rights-in-the-canadian-copyright-reform-process---jane-bailey; Jeffrey P. Cunard, "Technological Protection of Copyrighted Works and Copyrighted Management Systems: A Brief Survey of the Landscape" *ALAI Congress 2001*, www.alai-usa.org/2001_conference/pres_cunard.doc at 2; Michael Geist, "'TPMs': A perfect storm for consumers" *The Toronto Star* (31 Jan 2005), www.michaelgeist.ca/resc/html_bkup/jan312005.html; Canadian Internet Policy and Public Interest Clinic, Media Release, "CIPPIC Questions Unbalanced Copyright Bill" (20 June 2005), www.cippic.ca/documents/Media_Release_-_Copyright_Bill_-_20_June_05_Final.pdf; Charles Clark, "The Answer to the Machine is in the Machine," in Bernt Hugenholtz, ed., *The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloqium* (The Hague: Kluwer Law International, 1996); Garry L. Founds, "Shrink-wrap and Clickwrap Agreements: 2B or Not 2B?" (1999) 52 Fed. Comm. L.J. 99; Daniel B. Ravicher, "Facilitating Collaborative Software Development: The Enforceability of Mass-Market Public Software Licenses" (2000) 5 Va. J.L. & Tech. 11.

could be used in a systematic attempt to "automate human virtue" — programming people to "do the right thing" by constraining and in some cases altogether eliminating moral behaviour through technology rather than ethics or law. Originally introduced to improve the human condition, digital locks and other automation technologies could, ironically, be used to control our virtual and physical environments in unprecedented ways, to eliminate the possibility for moral deliberation about certain kinds of action otherwise possible in these spaces by disabling the world in a way that ultimately disables the people who populate it. Not by eliminating their choices but by automating them — by removing people from the realm of moral action altogether, thereby impairing their future moral development.

I begin in Section B with a series of historical and cultural vignettes investigating the nature, purpose and symbolic significance of locks. Recognizing that keys are in fact "the key" to a proper understanding of locking systems, I go on in Section C to examine digital locks and the power afforded to keyholders to control others through the automation of permissions, in effect enabling or disabling the world we live in by setting the terms and conditions for its use. Section D is where I illustrate this through a connected series of anecdotes from my own personal experience. Here, I sketch the potential progression of a widespread digital lock strategy through a series of developments in "carting" technologies and indicate what this might mean. In Section E, I ask how all of this might affect us as moral actors who desire to do good things. Examining Aristotle's account of virtue ethics, I demonstrate that a state sanctioned, unimpeded and widespread digital lock strategy would impair our moral development by impeding our ability and desire to cultivate the practical wisdom necessary for the acquisition of morally virtuous dispositions. Finally, in Section F, I briefly investigate Bill C-32, Canada's proposal for sanctioning the use of digital locks and prohibiting their circumvention. Arguing that the flaws in Bill C-32 are symptomatic of the larger digital lock strategy, I conclude that the proposed legislative solution is inelegant — a brute force formula that fails to achieve a balanced copyright framework. I suggest that those who use digital locks might sometimes owe a positive obligation to provide a key whenever someone else has a right to access or use the thing that has been locked-up. I further suggest that the laws protecting digital locks, like the digital and mechanical locks themselves, must be understood as something more than instruments of exclusion since a series of ubiquitous locks designed to keep people honest will in fact impair the development of a deep-seated disposition necessary for honesty.

B. LOCK AND KEY

Prior to the invention of locks, people, like animals, often buried their valuables, or hid them in caves or the trunks of trees.[20] This rather imperfect means of securing their belongings eventually gave way to innovation. As is evident from the legend of the Gordian knot, cords and ropes were initially used to tie things down. The strength and complexity of the Gordian knot, for instance, was used to physically hamper theft of the king's ox-cart by tethering it to a post firmly rooted in the ground. It was not long before it was discovered that knots could be used in other ways. For example, the "thief knot,"[21] was employed not to hamper but to monitor possible intruders by detecting whether property had been tampered with. This early technology was simple but ingenious.[22] The design of the thief knot very closely resembled the popular maritime "reef knot."[23] A sailor using this technique would "secure" his belongings in a ditty bag using the thief knot, often with the ends hidden.[24] If another sailor untied the knot and rifled through the bag — even if he took nothing — it was likely that he would re-tie the bag using the more common reef knot, revealing to the owner that the bag had been tampered with.[25]

While techniques such as these offered some measure of security, it was the advent of mechanical locks that truly changed the game. It is thought that the earliest locks were constructed approximately 4,000 years ago.[26] However, the first archaeological discovery of a wooden lock — now known as the "Egyptian door lock" — dates back to the reign of Sargon II, who is believed to have used this technology to secure his palace in Khorsabad, near Nineveh, where he reigned from 722 to 705 B.C.[27] Its basic mechanism was a large wooden bolt used to secure a door, which had a slot with

---

20 Access Key and Lock, "A Brief History of Locks," (2010) www.keyandlocksupplies.co.uk/80665/info.php?p=15 [Access Lock].

21 Colin Jarman, *Top Knots,* (London: Quintet Publishing, 2001) at 32–33. See also Lindsey Philpott, *Pocket Guide to Knots*, (Singapore: New Holland Publishers Ltd., 2006) at 158–59.

22 The underlying strategy of the thief knot is utilized to this day in modern cryptographic techniques.

23 Jarman, above note 21 at 32; Philpott, above note 21 at 158.

24 Jarman, *ibid*. at 40; Philpott, *ibid*. at 160.

25 This is because the thief knot unties itself if the lines are pulled when the same action would seize a reef knot.

26 The Keyless Lock Store, "Ancient Roman Key Gallery and a Brief History Lesson" (2010), www.nokey.com/ankeymus.html [Keyless Lock Store].

27 "Schlage's History of Locks!" Dafor OY, www.locks.ru/germ/informat/schlagehistory.htm [Schlage].

several holes in its upper surface. The holes were filled with wooden pegs that prevented the bolt from being opened.[28] The design enjoyed significant longevity and is in fact the forerunner to modern pin tumbler locking systems used today.[29]

The remainder of the lengthy but extremely interesting history of locks — from pin tumblers to warded locks to levers and double-acting levers to tubular locks to digital encryption[30] — can for present purposes be understood as a series of innovations spurred to some degree by the monetary incentives of the patent system but, for the most part, by the ever-escalating arms race between lock-makers and lock-breakers.[31] It is probably fair to say that, throughout the centuries, there are really only two basic means of securing mechanical locks. The first is "by means of fixed obstructions to prevent wrong keys from entering or turning in the locks. The other, which is superior, employs one or more movable detainers, which must be arranged in pre-selected positions by the key before the bolt will move."[32]

There is an old Irish proverb that says, "A lock is better than suspicion."[33] Locks offer an ability to exclude others. They seek to prevent others from exercising control over us, and our possessions. As the proverb suggests, locks are a reassuring alternative to the insecurity we can feel when our possessions remain vulnerable to the incursions of others. For this reason,

---

28 *Ibid.*

29 Lock and Key — History, (2010), http://science.jrank.org/pages/3989/Lock-Key-History.html.

30 The following websites provide similar accounts of the timeline of the development of locks: Keyless Lock Store, above note 26; *Schlage*, above note 27; Brian Morland, "The History of Locks Museum" *History of Locks*, www.historyoflocks.com [Lock Timeline].

31 There is a growing competitive movement called "locksport" that involves learning the theory of locks, analyzing the devices and figuring out ways to quickly defeat the systems without destroying them. These lockpickers thrive on the intellectual thrill of beating all sorts of locks, but oppose attempts to use the skill for mischievous purposes. "Competitive Lockpicking Growing in US Popularity" *NPR* (28 July, 2010), www.npr.org/templates/story/story.php?storyId=128815821. To learn more about the history of lock picking, please refer generally to "Secrets of Lock Picking" by Steven Hampton, as a great example of providing accessible information to anyone who is looking to learn how to pick locks. Steven Hampton, *Secrets of Lockpicking* (Boulder: Paladin Press, 1987).

32 Access Lock, above note 20.

33 In Irish Gaelic, the expression is: "*Is fearr glas ná amhras*." See Island Ireland, "Irish Proverbs with English Translations," http://islandireland.com/Pages/folk/sets/proverbs.html.

locks are historically and culturally understood to be a crucial and indispensable technological development in the protection of private property. Locks have a long and rich history of use in the attempt to prevent theft and destruction.[34] Not surprisingly, the popular understanding of the proper function of a lock is exclusion. Locks keep intruders out. Locks protect private property. Locks prevent wrongdoing.

Then again, there is an even older Yiddish expression that, "A lock is good only for an honest man."[35] In other words, a thief looks at a lock as an inconvenience but not necessarily as a form of prevention. A lock is unlikely to dissuade an unwavering lock-picker who has significant resources, skill, knowledge and time.[36] Especially if s/he believes that there is a legal right to defeat the lock. Locks have *never* been perfect technologies of exclusion. All locks can be defeated. Today, the Internet operates as a force multiplier in this respect by making it easy to share the means of defeating locks *en masse*.[37] Even though there are many custom-made locks, safes and security systems that are in fact quite difficult to defeat, considerations of efficiency, cost and convenience usually undermine the security that locks are meant to provide. As one expert in the field recently put it:

> there is a basic conflict between security and convenience in the lock field. For example, the use of high-security locks has been resisted by American car-makers because of the difficulties drivers would encounter in finding rare blanks and the machines to cut the keys. Most people talk security, but they really want convenience.[38]

Consequently, it is fair to say that our everyday use of mass market locks is part of a broader "security theatre" — the adoption of *apparent* security

---

34 Lock Timeline, above note 30.

35 See Kehillat Israel Reconstructionist Synagogue, "Yiddish Sayings, Proverbs, Phrases, Aphorisms, Curses, and Insults," http://kehillatisrael.net/docs/yiddish/yiddish_pr.htm.

36 Although, even a standard lock can hamper a lesser intruder, and the disturbance generated in circumventing a decent lock (e.g., breaking windows) will deter many would-be thieves, shifting their attacks to weaker targets.

37 One could spend days browsing tens of thousands of techniques on websites ranging from answer.com to YouTube. See, e.g., "Lock Pick Guide, How to Pick a Lock," www.lockpickguide.com; Lock Picking 101, "Lockpicking, Locksmithing, Locksport, Locks and Picks," /www.lockpicking101.com; Howcast, "How to Pick Any Padlock or Combination Lock," www.youtube.com/watch?v=rRcBNJMoFIw.

38 Quote attributed to Richard Berry, product development manager for Sargent Manufacturing Co. in New Haven, Conn. Quoted in Steven Ashley, "Under lock and key," (1993) 115 Mechanical Engineering 62 at 67.

measures in order to provide *the feeling* of improved security while doing considerably less than might be supposed to improve actual security.[39] In this sense, historical and present day use of standard locks can to some extent be understood as a kind of convention or ritual, a leap of faith in which we place unfounded trust in the mysterious mechanism of lock and key. Whether the lock is mechanical or conceptual, digital or analog, "we religiously follow this ritual, often many times each day, [though] few are fully aware of what mechanical forces have been activated, but we have fulfilled a very fundamental psychological need."[40] "Locking-up" allows us to go out into the world and carry out our daily routines with the *belief* that our homes and possessions are safe. In this respect, we are not unlike the ancients, who believed the iron used to make locks was *apotropeic* — counteracting the forces of evil and all malevolent spirits that tried to enter people's homes, churches, and storage areas through keyholes and other openings.[41]

The ritualistic aspect of "locking-up" is illustrated by a 700-year-old ceremony that still takes place every single night[42] in England at the Tower of London:

> Every night, at exactly seven minutes to 10 o'clock, the Chief Yeoman Warder of the Tower emerges from the Byward Tower wearing

39 The term security theatre has been used to describe the implementation of security initiatives that are palliative in nature. Such procedures are designed to reassure users that measures have been taken for their protection, often in response to a crisis or tragedy. Bruce Schneier describes security theatre as "countermeasures [that] provide the feeling of security instead of the reality." His examples include placing unarmed guards in airports following the 9/11 terrorist attacks and introducing tamper resistant packaging following the random Tylenol poisonings of 1982. Air travelers were comforted by the presence of guards and consumers were set at ease by the addition of a thin seal. The fact that either measure could be easily overcome was irrelevant; as Schneier explains, "[m]ost people are comforted by action, whether good or bad." See Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York: Copernicus Books, 2003) at 38–40.

40 Lock Timeline, above note 30.

41 "Protective Iron," History of Locks (22 January 2008), www.historicallocks.com/en/site/hl/Articles/Locks-and-keys-in-folklore/Protective-iron .

42 The single exception occurred during WWII during an air raid on London on 16 April 1941. After a number of incendiary bombs fell on the old Victorian guardroom just as the Chief Yeoman Warder came through the Bloody Tower archway, he stood up, dusted himself off and carried on. It is said that The Tower holds a letter from the Officer of the Guard apologizing to King George VI for the delay in the ceremony, along with a reply from the King which says that the Officer is not to be punished as the delay was due to enemy action. See Colonel E.H. Carkeet-James O.B.E., M.C., *His Majesty's Tower of London* (London: Staples Press Limited, 1950) at 48. See also "Ceremony of the Keys," www.trooping-the-colour.co.uk/keys/index.htm.

> his long red coat and Tudor bonnet. He carries in one hand a candle lantern and in the other hand the Queens Keys. With solemn tread he moves along Water Lane, to Traitor's Gate where his escort, provided by one of the duty regiments of Foot Guards, awaits him. He hands the lantern to an escorting soldier and the party moves to the outer gate. On the way, all guards and sentries salute the Queen's Keys. After locking the outer gate the Chief Yeoman Warder and escort retrace their steps. The great oak gates of the Middle and Byward Towers are locked in turn. They now return along Water lane towards Traitor's Gate where, in the shadows of the Bloody Tower archway, a sentry awaits.
>
> "Halt, who comes there?" the sentry barks.
>
> "The Keys!" answers the Chief Yeoman Warder.
>
> "Whose Keys?"
>
> "Queen Elizabeth's Keys"
>
> "Pass Queen Elizabeth's Keys" replies the sentry, "and all's well"
>
> The party then proceeds through the Bloody Tower archway and up towards the broadwalk steps where the main guard is drawn up. The Chief Yeoman Warder and escort halt at the foot of the steps and the officer in charge gives the command to the Guard and Escort to present arms. The Chief Yeoman Warder moves two paces forward, raises his Tudor bonnet high in the air and calls "God preserve Queen Elizabeth." The guard answers "Amen" exactly as the clock chimes ten and 'The Duty Drummer' sounds The Last Post on his bugle. The Chief Yeoman Warder takes the keys to the Queen's House and the guard is dismissed.[43]

Although there are several accounts of the origin of the key ceremony, the one offered on tours at the Tower of London explains that it was initiated by Richard II in response to mob violence during the Peasant Revolt of 1381, reminding us of the kind of devastation that can take place when our homes (and castles) are not adequately locked.[44] Indirectly, it also reminds us of the power afforded to the key-holder. Indeed, lock technolo-

---

43 *His Majesty's Tower of London*, *ibid*. at 48.

44 While several competing origin stories can be found on the Internet, anecdotal experience suggests that this is the origin story favoured by the Yeoman Guards at the Tower of London. See Marilynn Doore, "The Ceremony of the Keys at the Tower" *Suite 101* (28 December 2009), www.suite101.com/content/the-ceremony-of-the-keys-at-the-tower-a156218.

gies are not properly or adequately understood without simultaneously examining the role and significance of keys.

Technically speaking, a key is a piece of metal mechanically fashioned through the shape of its bit to match the pins, wards or levers in the locking apparatus. However, throughout history, keys have been regarded as much more than just a mechanism. Ancient Greek and Roman keys — like well-crafted statues or carvings — were elegant and artistic.[45] Often ornate and cast in bronze, keys were status symbols indicating that their possessor had property worth protecting.[46] In ancient times, the number of keys a person owned was a measure of his importance as the head of a household.[47] Keys were large and cumbersome and slaves were often needed to carry them all. Having several key bearers indicated a person of great wealth and distinction.[48]

Of course, the symbolism of keys transcends wealth and stature. Conceptually, it is crucial to remember that keys not only lock — they unlock. Keys are therefore a "symbol of all forces that open and close, bind and release."[49] From this perspective it is wrongheaded to understand lock technologies merely as instruments of private property. The power of the key includes the power to exclude. But, surely, it is much more than that. *Keys give us the power to open or close, to turn on or turn off, to grant or deny, to allow or forbid.*

These broader social powers are represented across various cultural domains. For example, several classical paintings portray Christ handing Peter the keys to the kingdom of heaven.[50] Catholic teachings have inter-

---

45 World cultures have afforded considerable clout to locks and keys throughout the ages. For example, in China, miniature padlocks were traditionally given to newborn babies as a talisman. Animal-shaped padlocks would be used to convey messages. A fish padlock is always on guard, since fish sleep with their eyes open; an elephant padlock connotes strength. Ceremonial padlocks were also placed around the waists of expectant mothers, with a knotted cord being placed around a pregnant woman, which would remain until another ceremony in the ninth month. See "Ancient Style Padlocks," *History of Locks*, www.historyoflocks.com/padlo02.html#secret.

46 "History of Keys" Historical Locks (23 November 2007), www.historicallocks.com/en/site/hl/Articles/HistoryAboutLocks/History-of-keys.

47 *Schlage*, above note 27. Gender specific language is, unfortunately, intentional.

48 *Ibid.*

49 "Definition of keys," *Historical Locks*, (12 January 2008), www.historicallocks.com/en/site/hl/AboutHistoricalLocks/Definition-of-keys/.

50 This often-used illustration comes from bible verse Matthew 16:18–20: "I tell you that you are Peter, and on this rock I will build my church, and the gates of Hell will not overcome it. I will give you the keys of the kingdom of heaven; whatever

preted this to mean not that St. Peter would act as gatekeeper of heaven, but instead as his clout over the church on Earth. Indeed, the succession of the papacy has been referred to as the "passing of the keys,"[51] as the ruling Pope assumes Peter's authority to serve as interpreter of the word of God, for "whatever Peter 'binds' as a legal obligation on Earth is bound in heaven; whatever he looses in loosed in heaven."[52] The "power of the keys," in this context, has been interpreted to include the very real and highly political power to admit or exclude from church membership, to set church policy and teachings, to render binding interpretations of sacred scripture, and to bind and loose sins.[53]

Heavenly destinations aside, keys to the gates of a city also carried significant symbolic power through until at least the 18th century.[54] By keeping unwanted strangers out, the keys to the city represented its inhabitants' right to security and self-determination.[55] The surrender of a city to an attacking army was historically symbolized by turning over

---

you bind on earth will be bound in heaven, and whatever you loose on earth will be loosed in heaven." Famous depictions include the fresco "Christ Giving the Keys to St. Peter" in the Sistine Chapel by Pietro Perugino and "The Delivery of the Keys to St. Peter" by Bernardo Strozzi. See Peter Perugino, "Frescoes on the side walls of the Sistine Chapel" *Web Gallery of Art*, www.wga.hu/frames-e.html?/html/p/perugino/sistina/index.html; "European: 1600–1800" *Chazen Museum of Art* (2005), http://chazen.wisc.edu/collection/paintings/euro_pt2.htm#.

51 See generally Francis A. Burkle-Young, *Passing the Keys: Modern Cardinals, Conclaves, and the Election of the Next Pope* (Oxford: Madison Books, 1999).

52 Richard P. McBrien, *The HarperCollins Encyclopedia of Catholicism*, (New York: HarperCollins Publishers Inc., 1995) *s.v.* "keys, power of the" at 735.

53 *New Catholic Encyclopedia,* Vol. 8, (Washington: The Catholic University of America, 1967) *s.v.* "Keys, Power Of" at 172.

54 Indeed "key to the city" ceremonies take place to this day as a way of honouring individuals for significant accomplishments. For example, Harry Winkler, better known to television audiences as Arthur "The Fonz" Fonzarelli of television's hit 70s TV show *Happy Days* currently holds the keys to the cities of Dallas, New Orleans, and Winnipeg. According to news reports, Winkler grew up with undiagnosed dyslexia and has since gained recognition as a children's author, a source of inspiration for those with learning disabilities. Winnipeg mayor Sam Katz admits that bestowing this honour upon Winkler was spurred by most young men in the 1970s who wanted to wake up to be as cool as "The Fonz." See "Fonzie gets key to the city" *CBC News Canada* (26 March 2010), www.cbc.ca/canada/manitoba/story/2010/03/26/mb-winkler-fonz-key-winnipeg.html. See also "Actor who played The Fonz on "Happy Days" receives key to Winnipeg city" *CTV Edmonton* (29 March 2010) http://edmonton.ctv.ca/servlet/an/local/CTVNews/20100329/100329_happydays/20100329/?hub=CP24Entertainment.

55 "The Keys to the City" *Historical Locks* (22 January 2008), www.historicallocks.com/en/site/hl/Articles/Locks-and-keys-in-art/The-keys-to-the-city.

its keys to the conquerors. In one classic example, the Bayeux tapestry portrays the Duke Conan ensnared within the tower of the city and despairingly handing over the keys to the castle of Dinan to William the Conqueror.[56] Similarly, the Spanish painter Velázquez's famous portrait of "The Surrender of Breda (1625)" celebrates the Dutch governor of Breda meekly handing over the key to the city to Spanish general Ambrosio de Spinola.[57] Ironically, Spanish culture did not always have a great deal of trust in locks and keys. At a later point in its history, householders would hire a watchman to invigilate their neighbourhood, who would carry at once the keys to all of the dwellings in that neighbourhood. To enter or leave a house, residents would clap to summon the watchman, such that all comings and goings became a matter of public record.[58] In this context, locks enabled personal privacy, while control of the keys by a trusted third party offered accountability.[59]

While this last example suggests that in the broader security context lock and key are flipsides of the same coin, most historical and technological accounts tend to focus on the lock alone. This is potentially problematic when the ultimate goal is to develop law and policies about locks. The narrower focus on locks creates a misperception in most lay people — *including those responsible for drafting the so-called "digital lock" provisions in Canada's copyright reform bill (*Bill C-32*)* — who come to think of locks, narrowly, as mere instruments of exclusion used to protect private property.

While locks can and do perform this function, our brief consideration of the significance of keys suggests a richer understanding of the nature and function of locking technologies. This more robust understanding of locking mechanisms recognizes symbolic and actual power stemming not from the fact that these mechanisms can be locked but, rather, that they

---

56 On plate 26 of the tapestry, the defenders of the castle of Dinan are pictured resisting the invading Norman troops, while the Normans set fire to the castle. Then Conan surrenders, and transfers they keys of the castle from his lance to William's. See Sir Frank Stenton, ed., *The Bayeux Tapestry: A Comprehensive Survey* (London: Phaidon Press, 1957).

57 Pedro Marrades, *Velázquez Y Su Siglo* (Madrid: Espasa-Calpe, S.A., 1953) at 347. See also Robert Harvard, *The Spanish Eye Painters and Poets of Spain* (Woodbridge: Tamesis, 2007) at 33.

58 *Schlage*, above note 27.

59 Not much has changed in the digital realm, where trusted third parties are used in public key infrastructures (PKI) to authenticate transactions through the creation, management, distribution, use, storage, and revocation of digital certificates. See Carlisle Adams & Steve Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*, 2d ed. (Boston: Pearson Education, Inc., 2003).

can be unlocked. The fact that locks are *made* to be unlocked suggests that, unlike other security barriers, the essence of their design is not simple or systematic exclusion, but something else. From the perspective of the intended key-holder, locks provide an access-control device that is premised on the notion of appropriate or authorized permission.

Although this point is not commonly acknowledged in typical discussions of locks, it is certainly well known by those working in the security field. Here is how security expert, Bruce Schneier, articulates this point in his leading text, *Beyond Fear*:

> The problem with securing assets and their functionality is that, by definition, you don't want to protect them from everybody. It makes no sense to protect assets from their owner, or from other authorized individuals (including the trusted personnel who maintain the security system). In effect, then, all security systems need to allow people in, even as they keep people out. Designing a security system that accurately identifies, authenticates, and authorizes trusted individuals is highly complex and filled with nuance, but critical to security.
>
> It's not sufficient to protect a valuable asset by encasing it in stone or steel, or by sending it to outer space, or by posting armed guards around it. With a very few exceptions, all security barriers need to be penetrated — under authorized circumstances by trusted people. The barrier needs a system that facilitates penetration, and additional systems to determine who is trusted. Buildings and safes have doors and keys or combinations so authorized people can open them. A casino slot machine has a locked door that lets maintenance personnel repair and refill the machine; it also has an opening through which players can collect their winnings — another avenue of penetration, for the user who has been temporarily "authorized" by a winning spin.
>
> The additional security requirements needed to make a barrier conditionally penetrable necessitate an enormous effort of planning, design, and execution: What was once a simple system becomes a complex one. A barrier is designed to keep attackers out; but since we need to allow people in, we must make a barrier that can be penetrated in authorized circumstances and can't be penetrated under any other circumstances. We need to punch a hole in the barrier and then control access to that hole. Our intentionally created holes — windows and doors, for example — are far and away the most frequent avenues for unauthorized entry. The holes we intentionally put in a

> barrier are very often the weakest link, since they make the security of the barrier depend on the security of the hole and its own systems: identifying the trusted people who are allowed in, the circumstances under which they are to be allowed in, and what privileges they are to have once inside. These ancillary systems of identification, authentication, and authorization are far more complex and subtle than they seem. Understanding the security of barriers means understanding the security of these systems.[60]

As Schneier's lengthy passages reveal, locks are as much technologies of permission as they are technologies of exclusion. The best locking systems not only prevent access to interlopers but also grant access to those who have or ought to have permission. This cannot easily be achieved with a typical mechanical lock since it is difficult to ensure that its key-holder always has permission.[61] This is where digital locks are thought to come into play. Whereas the point of a mechanical lock is to guarantee the key-holder automatic entry, the more sophisticated digital locks automate the actual permission with stunning precision. As will be discussed in the section that follows, digital locks can be used in conjunction with automated identification and authentication systems to ensure that the key-holder is, or ought to be, authorized to do whatever the lock would otherwise preclude. But, as we shall also see, digital locks can do much more than that.

C. DIGITAL LOCKS

Not surprisingly, the invention of digital locks coincided with the advent of digital property. Digital locks are Gordian knots for content owners, a digital antidote to Stewart Brand's famous revelation that "information wants to be free":

> Information wants to be free. Information also wants to be expensive. Information wants to be free because it has become so cheap to distribute, copy, and recombine — too cheap to meter. It wants to be expensive because it can be immeasurably valuable to the recipient. That tension will not go away. It leads to endless wrenching debate about price, copyright, "intellectual property," the moral rightness

60 Schneier, above note 39 at 181.

61 Since keys can be taken by force, forged, found or can be shared without permission.

> of casual distribution, because each round of new devices makes the tension worse, not better.[62]

Digital locks are the newest round of devices, and the tension Brand refers to is not only the escalating technological arms race between digital lock-maker and lock-breaker but also the legal clash between those who would seek further protection of digital locks through legislation and those concerned about the broader social consequences of doing so. Disentangling the technological from the legal is difficult and to some extent artificial, especially in light of the World Intellectual Property Organization's (WIPO) global imperative to provide legal protection to digital locks[63] and the new role that digital locks sometimes play in hybrid techno-legal systems discussed below, known as DRM. Because many others[64] and I[65] have

---

62 Stewart Brand, *The Media Lab: Inventing the Future at MIT* (New York: Viking Penguin Inc., 1987) at 202.

63 Both of the 1996 World Intellectual Property Organization (WIPO) treaties, and the forthcoming Anti-Counterfeiting Trade Agreement (ACTA), include provisions that enhance digital locks through guaranteeing legal protections. In particular, conforming to the requirements of the WIPO treaties is often cited as rationale for increasing domestic protection for technological protection measures. The relevant provisions are Article 11 in the *WIPO Copyright Treaty* and Article 18 in the *WIPO Performances and Phonograms Treaty*. See *WIPO Copyright Treaty*, 20 December 1996, (1997) 36 I.L.M. 65 (entered into force 6 March 2002), www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html, art. 11 [*WCT*]; Article 18, *WIPO Performances and Phonograms Treaty*, 20 December 1996, (1997) 36 I.L.M. 76, (entered into force 20 May 2002), www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html, art. 18 [*WPPT*].

64 Above note 12 and accompanying text.

65 Ian Kerr, "If Left To Their Own Devices: How DRM and Anti-circumvention Laws Can Be Used to Hack Privacy" in Michael Geist, ed., *In The Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005) 167 www.irwinlaw.com/store/product/120/in-the-public-interest--the-future-of-canadian-copyright-law [*If Left To Their Own Devices*]; Ian Kerr & Jane Bailey, "The Implications of Digital Rights Management for Privacy and Freedom of Expression" (2004) 2:1 Information, Communication & Ethics in Society 87; Ian Kerr, Alana Maurushat, & Chris Tacit, "Technical Protection Measures: Tilting at Copyright's Windmill" (2002) 34:7 Ottawa L. Rev. 13; Ian Kerr, Alana Maurushat, & Chris Tacit, "Technological Protection Measures: Part I — Trends in Technical Protection Measures and Circumvention Technologies" (2004) Department of Canadian Heritage, Copyright Policy Branch, http://ssrn.com/abstract=705003 [*Heritage Report Part I*]; Ian Kerr, Alana Maurushat, & Chris Tacit, "Technical Protection Measures: Part II — The Legal Protection of TPMs" (2004) Department of Canadian Heritage, Copyright Policy Branch, http://ssrn.com/abstract=705081 [*Heritage Report Part II*]; Ian Kerr, "To OBSERVE AND PROTECT? How Digital Rights Management Systems Threaten Privacy and What Policy Makers Should Do About It" in Peter Yu, ed., *Intellectual Property and Information Wealth: Copyright and Related Rights*, vol. 1 (Westport: Praeger Publishers, 2007).

already written extensively on these broader subjects, my aim in this section[66] is limited to a brief description of digital locks and DRM, with a particular focus on their role in what I call "the automation of permissions."

Although digital lock technologies offer an imponderable number of powerful applications across various domains,[67] their early and current use has been driven primarily by the copyright industries. In the copyright context, digital locks are often encoded within software, films, music, books, games and other digital media. The "digital lock" metaphor is colloquial and provocative no matter what side of the "copyfight" fence you sit on. Not long after this and other phrases entered the public lexicon, WIPO and other like-minded stakeholders sought a more neutral linguistic terrain. Through their efforts[68] the term "technological protection measure"[69] or, TPM, has been adopted as the global signifier for the technique of locking-up a digital work.

In its simplest form, a TPM is a technical method employed to control access to work subject to copyright, or to control its subsequent use.[70] While at first blush this might seem similar in effect to the proverbial lock on the cupboard, TPMs enable an incredibly nuanced level of access control as well as a fine-grained ability to monitor and manage the way that

---

66 Portions of this section are adapted from my own previous writing on the subject, including my co-authored studies for the Department of Canadian Heritage: Ian Kerr, Alana Maurushat, & Chris Tacit, "Technological Protection Measures: Part I — Trends in Technical Protection Measures and Circumvention Technologies" (2004) Department of Canadian Heritage, Copyright Policy Branch, http://ssrn.com/abstract=705003; Ian Kerr, Alana Maurushat, & Chris Tacit, "Technical Protection Measures: Part II — The Legal Protection of TPMs" (2004) Department of Canadian Heritage, Copyright Policy Branch, http://ssrn.com/abstract=705081; and a book chapter written for Michael Geist's previous study of copyright reform in Canada: Ian Kerr, "If Left To Their Own Devices: How DRM and Anti-circumvention Laws Can Be Used to Hack Privacy" in Michael Geist, ed., *In The Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005) 167, www.irwinlaw.com/content/assets/content-commons/120/Two_03_Kerr.pdf .

67 I shall provide some stark examples in the following sections.

68 *WCT* above note 60; *WPPT* above note 60.

69 They are sometimes also referred to as "technical protection measures."

70 This includes: copying, distribution, performance, and display. See Perry, above note 12. Canada's recently proposed Bill C-32 defines a TPM as "any effective technology, device or component that, in the ordinary course of its operation, (a) controls access to a work, to a performer's performance fixed in a sound recording or to a sound recording and whose use is authorized by the copyright owner; or (b) restricts the doing — with respect to a work, to a performer's performance fixed in a sound recording or to a sound recording — of any act referred to in section 3, 15 or 18 and any act for which remuneration is payable under section 19." See Bill C-32, above note 10.

digital property is used. For example, techniques have been developed in the field of cryptography to link encrypted files to devices or players comprised of hardware or software so that an encrypted message can only be decrypted using that particular device or player.[71] This is what allows companies like Apple to control the kinds of applications that can operate on their devices[72] and, to some extent, the kind of content.[73] It also allows digital content to be tethered to a particular device or player for a particular period of time.

Perhaps the best current example of this is the e-book, the increasingly widespread use of which has constituted a so-called "revolution."[74] More and more, consumers are attracted to this modern spin on an age-old pastime. There is something compelling in the advertising campaign for the

71 C. Risher, "Technological protection measures (anti-circumvention devices) and their relation to exceptions to copyright in the Electronic environment" (paper presented to the IPA Copyright Forum Frankfurt Book Fair, 20 October 2000) [unpublished].

72 Despite its business model of allowing developers to design and customize applications for the iPhone, Apple retains the ability to remove an application. Jonathan Zittrain has described this practice as "tethering," raising concerns about external control and autonomy. See Jonathan Zittrain, "The iPhone Kill Switch" *The Future of the Internet and How to Stop It*, (14 August 2008), http://futureoftheinternet.org/the-iphone-kill-switch; see also Brad Stone, "Amazon Faces a Fight Over Its E-Books" *The New York Times Online* (26 July 2009), www.nytimes.com/2009/07/27/technology/companies/27amazon.html.

73 For example, Apple CEO Steve Jobs has decreed that Apple products such as the iPad and iPhone will not run Flash-based applications. The official rationale for this decree includes concerns about reliability, prolonging battery life on mobile devices, and most importantly, reliance on cross-platform development tools hindering the creation of Apple-specific products. Another reason for this decision, revealed in an email debate with Gawker.com writer Ryan Tate, is that eliminating Flash offers users "freedom from porn," since most web-based pornographic videos use the Flash platform. For Apple's official stance on Adobe Flash, see Steve Jobs, "Thoughts on Flash" *Apple.com* (April 2010), www.apple.com/hotnews/thoughts-on-flash/. For the origin of the phrase "freedom from porn," see Ryan Tate, "Steve Jobs Offers World Freedom From Porn" *ValleyWag* (15 May 2010), http://gawker.com/5539717/steve-jobs-offers-world-freedom-from-porn.

74 For use of the phrase "eBook revolution," see Mike Elgan, "Here comes the e-book revolution" *Computerworld* (7 February 2009), www.computerworld.com/s/article/9127538/Elgan_Here_comes_the_e_book_revolution. See also John Anderson, "The Ebook Revolution is Irreversible: Digitization is Replacing Physical Publishing" *Suite 101* (24 February 2010), http://bookpublishing.suite101.com/article.cfm/the-ebook-revolution-is-irreversible.

Kindle: "Think of a book and start reading it in 60 seconds."[75] It doesn't hurt that you can also carry around 3,500 e-books all at once. Despite Steve Jobs' (since repressed) assertion that no one reads anymore,[76] e-books have become the format of choice for many and are stretching the boundaries of the written word. Convenience, economic incentives, aggressive online marketing campaigns, and environmental concerns tied to saving paper have all been given as reasons to embrace e-books.[77] Younger consumers who have grown up in the digital age and may have felt disenfranchised by old-fashioned books are embracing this new medium with fervor. And the revolution is not only in form but also in substance. E-books have the potential to change not only the way consumers view their books, but also the content of the books themselves. As electronic formats are adopted, it is likely that books will be adapted to better suit these new formats: shorter, timelier, more culturally relevant.[78] For example, in Japan and South Korea, where cell phone use is ubiquitous, so is the cell phone novella.[79]

With an increasing consumption of literary and artistic works in a digitized form comes the spectre of external control through TPMs. Here, Jonathan Zittrain's description of Apple's products as "tethered appliances" rings true.[80] As we shall see, this raises questions about what it means to say that a consumer has 'purchased' a book, a song or a movie.

Consider the evolving business model for renting movies. Under the older system of going to a store to rent plastic discs, though it would be inconvenient for the average customer to make illegal copies of those disks, the customer was at liberty to play the movie wherever[81] and as often and

---

75 Jeff Bezos, "Amazon Debuts a 3G Kindle, and That's Only Half of Jeff's News," *[e-reads]*, (29 July 2010) http://ereads.com/2010/07/amazon-debuts-gen-3-kindle-and-thats-only-half-of-jeffs-news.html.

76 Well, he said it! This was his first response to the launch of Amazon's Kindle (his second response being the e-book app for his iPad). See John Markoff, "The Passion of Steve Jobs" *The New York Times* (15 January 2008), http://bits.blogs.nytimes.com/2008/01/15/the-passion-of-steve-jobs/; see also Michael Wolf, "iPad Fueling Enhanced E-Book Revolution" *Gigaom* (21 July 2010), http://gigaom.com/2010/07/21/ipad-fueling-enhanced-e-book-revolution/.

77 Mike Elgan, "Here comes the e-book revolution" *Computerworld* (7 February 2009), www.computerworld.com/s/article/9127538/Elgan_Here_comes_the_e_book_revolution.

78 *Ibid.*

79 *Ibid.* See also William Patry, *Moral Panics and the Copyright Wars* (New York: Oxford University Press, 2009) at 195.

80 Zittrain, above note 72.

81 Subject to regional coding. See e.g., "DVD Regions," www.amazon.co.uk/gp/help/customer/display.html?nodeId=502554. See also "DVD Regions" *Home Theatre Info*, www.hometheaterinfo.com/dvd3.htm.

for as long as she or he wishes, subject to late penalties at the store. Customers not only had the freedom to consume the product however they wished during the rental period but also to share it with others. Using TPMs such as the encryption techniques described above, the movie rental, now downloaded from an online v-tailer, can be limited to the machine used for downloading and can also be programmed to be deleted from that machine at a specified time or, in some cases, at the content owner's whim. Unlike the simple binary (open/close) nature of the analog lock on the neighbourhood video store's door, the level of control afforded by the digital lock puts the content owner/provider, rather than the customer, in the driver's seat. Continuing with the above example, if you did not have a chance to watch the movie you rented before its preset expiry date, or if you wished to keep it a day longer to show it to your roommate the next night,[82] you no longer have the option of simply keeping it and paying late fees. The movie is automatically disabled (or deleted) and can no longer be viewed by your player.

What this example reveals is that TPMs are in fact much more than a lock in digital clothing. The metaphor of the lock is not nearly strong enough to convey the full power of TPMs. This is one of the reasons why proposals to give digital locks further legal protection is so controversial. TPMs already afford copyright owners protection beyond that which would have been guaranteed by copyright law alone. As Professor Carys Craig has recently described it:

> Activities such as reading, listening, and viewing have always been perfectly lawful — and of course desirable from a cultural policy perspective — in the analogue world. *Nothing in the law of copyright would prohibit* someone from flipping through a magazine in a doctor's office, borrowing a novel from a friend, listening to a roommate's music collection, or watching a movie on a home video machine.[83]

---

82 But not until she finished her work slavishly formatting footnotes for her professor! I am grateful to Katie Szilagyi and Shea Loewen for sharing their painful experience of this with me, even though good fortune would have it that the movie in question didn't quite live up to the book upon which it was based. (Alas, a different kind of copyright problem . . .)

83 Carys J. Craig, "Digital Locks and the Fate of Fair Dealing in Canada: In Pursuit of Prescriptive Parallelism" (2010) 13 J. World Intellectual Property 503 at 9 [emphasis added].

Professor Craig's point is important to any legitimate attempt at balanced copyright.[84] But what I like most about the above passage is that its subtle phrasing ("nothing in the law of copyright would prohibit. . .") hints at a far more significant point that has not been carefully articulated in the current literature on digital locks. For starters, TPMs — unlike copyright law — would prohibit, in a digital context, activities that we consider commonplace in the analog world, such as "flipping through a magazine in a doctor's office, borrowing a novel from a friend, listening to a roommate's music collection, or watching a movie on a home video machine."[85]

But, here is the crucial point: by prohibiting these things, TPMs have the ability to radically shift copyright's defaults by automating its system of permissions. Prior to the advent of TPMs, the default for intellectual consumption might have been explained to lay persons through the heuristic of an old adage — "sometimes, it is better to beg for forgiveness than to ask for permission." While obviously hyperbolic and totally inaccurate as an actual statement of the law of intellectual property, in terms of copyright's underlying intellectual consumption defaults, the adage does illustrate the fact that citizens, as consumers, are generally at liberty to consume intellectual products as they think is fair, except to the extent that a content owner subsequently asserts that such consumption is in breach of its copyrights. Citizens are not generally required[86] to ask content owners or anyone else for *prior permission* every time that they wish to gain access to, read, share or otherwise use someone else's intellectual work (especially those that they have already purchased). This kind of copyright clearance *en masse* would not only fly in the face of fair-

---

84 As she goes on to say at page 13: "This is the challenge that now presents itself to policy-makers and the Canadian copyright system: how can copyright's delicate balancing act continue to be performed in any meaningful way when the technological environment is increasingly one of absolutes — absolute freedom versus absolute control." *Ibid*.

85 *Ibid*.

86 Although the above is still generally true, there is an expanding resistance by content owners aimed at thwarting a creative process known as "remixing" (the attempt to integrate, change, improve upon or in some other way remake a work that is subject to copyright). According to Professor Lessig, the response by copyright industries seeks to promote what he calls a *permission culture*: "The opposite of a free culture is a "permission culture" — a culture in which creators get to create only with the permission of the powerful, or of creators from the past." Lessig, above at note 11 at xiv. Digital locks, he thinks, help to ensure that "we are less and less a free culture, more and more a permission culture." Lessig, above at note 11 at 8; See also, Lawrence Lessig, *Remix: Making Art and Commerce Thrive In The Hybrid Economy* (New York: The Penguin Press, 2008).

dealing principles and other user rights, it would cripple most systems of distribution currently in place. That said, in cases where people exceed their rights as users and forgiveness is *not* forthcoming, content owners obviously have the right to seek remedies for copyright infringement by way of legal action.

The digital lock strategy effectively seeks to reverse these intellectual consumption defaults through its automation of permissions. In the case of digital locks it is no longer better to ask for forgiveness (or pay the penalty) since there is no longer anything to forgive or to be penalized for. Returning once again to the movie rental example from above, deliberation over a decision (not) to keep the movie for an extra day is no longer an option. With digital locks, your ability to wait until later to watch the movie that you already rented and paid for is only available by *prior permission*.

Recall, now, my argument in the previous section — that locks are as much technologies of permission as they are technologies of exclusion. Shown in their very best light, TPMs can be used to ensure appropriate or authorized permission. However, as the above examples (and others that will follow) suggest, TPMs can go well beyond appropriate or authorized permission. In fact, TPMs can be employed in even more sophisticated DRMs to automate *all* permissions, shutting down any and every possible course of action except for those pre-selected by the party employing the digital lock. While TPMs might be thought of as the building blocks used to restrict access or use, DRMs are designed to manage an entire array of related activities by using various automation and surveillance technologies to identify digital property and those seeking to use it, in order to technologically enforce certain licensing conditions. In so doing, DRM can be used to automate permission systematically.

In the copyright context, these systems can be used to track royalties or run accounting systems that monitor usage and payment. They enable business models that go beyond sales and subscriptions, including licensing arrangements with variable terms and conditions. But the DRM strategy extends well beyond copyright. More generally, DRM can refer to any "technology systems facilitating the trusted and dynamic management of rights in any kind of digital information, throughout its life cycle, irrespective of how and where the digital information is distributed."[87]

---

87 Nic Garnett, "Outline of Presentation of Nic Garnett, representing InterTrust Technologies" (paper presented to the ALAI Congress 2001, June 2001) [unpublished], www.alai-usa.org/2001_conference/pres_garnett.doc at 1. This is a fairly broad definition of DRMs for, as the author notes, "the term DRM has now come to be applied

Typically, a DRM consists of two components. The first component is a set of technologies that could include encryption, authentication, access control, digital watermarking, tamper-resistant hardware and software, and risk management architectures. In the copyright context, such technologies are used to enforce corporate copyright policies and pricing schemes through a registration process that requires purchasers to hand over certain bits of personal information. The second component is a licensing arrangement. This set of legal permissions establishes the terms of use for the digital property by way of contract.[88]

If a TPM is a virtual fence, then a DRM is a virtual surveillance system. The technological components of most full-blown DRMs are linked to a database, which enables the automated collection and exchange of various kinds of information among rights owners and distributors, about the particular people who use their products. This includes users' identities, their habits, and their particular uses of the digital material subject to copyright. The information collected can be employed in a number of ways that go well beyond ensuring access and use that is authorized by copyright laws. As we have seen, DRM-enabled movie players can limit the ability to copy the digital work, restrict its transmission to other users, prevent or limit its transfer to machines other than the one on which it is registered to run, and even set limits on the number of times that the work can be accessed.[89] In the course of its normal operation, a DRM can even be used to track and record the various uses of works. Consequently, and perhaps most importantly, DRM can be used not only to enforce the rights accorded to content owners pursuant to copyright statutes but can also be used to set entirely new ground rules, giving even more rights to property owners in accordance with the rules that they have set for themselves in the terms and conditions of the licensing arrangement accompanying the DRM, usually on a take-it-or-leave-it basis.[90]

---

to a variety of different technologies, most of which relate to the control of access to information or to its copying."

88 Gervais, above note 12. Hugenholtz has defined a DRM similarly as a contract, typically a licensing agreement, coupled with technology, typically a technological protection measure such as encryption. See Hugenholtz, above note 12.

89 For a complete overview of the attributes of DRMs, see Gervais, above note 12.

90 Jeffrey P. Cunard, "Technological Protection of Copyrighted Works and Copyrighted Management Systems: A Brief Survey of the Landscape" (paper presented to the ALAI Congress, June 2001) [unpublished], www.alai-usa.org/2001_conference/pres_cunard.doc at 2.

The ability to change the ground rules in this way affords tremendous power to those in a position to employ DRM. Purchasers of Amazon's e-book reader, the Kindle, experienced this power first hand in the summer of 2009 after many law-abiding readers who had legally purchased from Amazon copies of George Orwell's *1984* and *Animal Farm* had those titles auto-deleted from their devices without their consent. According to news reports, Amazon mistook a "no" for a "yes" regarding a publisher's decision to extend its permission to publish Orwell's works in e-book format. Fearing serious sanction from the copyright owners after already having sold many e-copies, Amazon capitulated. Using the power of DRM to change the ground rules, Amazon was able to enter the private digital libraries of their many Kindle customers, to scan all of the titles on each and every active Kindle, and electronically seize the two Orwell books from all those who possessed them. Ironically, it was a classic Orwellian moment. Without a formal recall and without having to make a plea to customers to delete the book, with just a simple mouse click, "The Ministry of Truth" expunged the offending material without notice or permission, rectifying what it perceived as a mistaken past by replacing it with a perfected present.

Other than the irony of deleting Orwell's books without consent and contrary to the licensing agreement, Amazon's DRM is not unusual. As is true in most DRM-enabled distribution systems, the ongoing exchange of personal usage information between user-owned devices and content owner/provider servers takes place in an invisible "handshake" occurring in the software layer. This allows for the transmission of personal usage information from the devices that we own back to the content owner/provider — something Professor Graham Greenleaf cleverly and famously characterized as "IP phone home."[91] The surveillance features associated with the database are crucial to the technological enforcement of the licensing component of the DRM. It is through the collection and storage of personal usage information that DRMs are able to "authorize use" in accordance with the terms of the licensing agreement thereby "managing copyrights." In the Amazon case, "authorizing use" is presumably what allowed Amazon to mistakenly sell those e-books to its customers for profit. "Managing copyright," on the other hand, seemed to include the powers necessary to rectify that mistake, such as snooping customers' book-

91 Graham Greenleaf, "IP, Phone Home: The Uneasy Relationship between Copyright and Privacy, Illustrated in the Laws of Hong Kong and Australia" (2002) 32 Hong Kong Law Journal 35 http://papers.ssrn.com/sol3/papers.cfm? abstract_id=884329.

shelves and auto-deleting digital property that they legally purchased at the content owner's whim.[92]

Although debacles of this sort rightly tempt critics to focus on DRM's potential for egregious breaches of privacy, access to information, personal autonomy and so forth, my current aim is to demonstrate that there is something much more fundamental at stake. I say this not because the digital locks on DVDs or the Kindle are primitive prototypes of what is likely to come. I say it because these are rather insignificant one-off examples compared to the potential social consequences of a more generalized strategy that uses digital locks to automate permissions writ large. In the next section, I will try to paint a picture of the gradual evolution of a widespread digital lock strategy and what it might mean.

D. CARTING

My concern is not with one kind digital lock technology versus another. Nor is my goal to shock-and-awe by portraying some dystopic digital lockdown. My aim is more straightforward. Through a reflection of my own anecdotal experiences, I want to try to imagine what would happen if we were to generalize copyright's digital lock strategy across other property-based domains. What affect would this have on fundamental legal institutions? And, how might it affect us as moral actors?

In thinking our way through moral problems the great philosopher, Immanuel Kant, famously suggested that we adopt a "categorical imperative" so that we "act only in accordance with that maxim through which you can at the same time will that it become a universal law."[93] In our current context we ask: what would it mean to will a universal adoption of a state sanctioned, unimpeded use of digital locks across all property-based domains? To set the stage for answering this question, I have very purposely chosen a low-tech, fairly simple form of property — the cart. In tracking a mere snapshot if its evolution, the carting example is offered as a heuristic

92 During all of this, Jeff Bezos, CEO of Amazon, groveled to his consumer base, admitting that its actions were "stupid, thoughtless, and painfully out of line with our principles." He promised that Amazon would "use the scar tissue from this painful mistake to help make better decisions going forward." What he didn't promise was to remove the DRM or rewrite its licensing conditions so that the auto-delete functionality is no longer possible. See Ian Kerr, "Robot law is taking over," *The Ottawa Citizen* (15 September 2009) http://iankerr.ca/index.php?view=article&catid=1:latest&id=749:robot-law-is-taking-over&format=pdf.

93 Immanuel Kant, *Foundations of the Metaphysics of Morals*, trans. by Lewis White Beck (Indianapolis: The Bobbs-Merrill Company, Inc., 1969) at 44.

for envisioning a world wherein the digital lock strategy is adopted much more broadly and then pondering its potential social implications.

Recall that it was King Gordius' famous ox-cart that inspired his son Midas to tie the Gordian knot. Other than its significance in terms of the prophecy of the oracle of Telmissus, one imagines this cart to have been fairly typical, a vehicle with wheels designed to transport items too heavy to carry. As described previously, the king's ox-cart was moored to a post within the palace grounds, preventing anyone unwilling or unable to untie it from moving it very far. Although carts are not always as valuable as the things they are meant to transport, the historic desire to control their use carries forward to present day.

Toy wagons aside, my own experience with carts probably began in my early childhood during a family vacation to Disneyland in the 1970s. Not ironically, this theme park, built in the 1950s and located about 45 minutes from Hollywood, was a key feature of Walt Disney's intellectual property strategy. My favorite part of the Magic Kingdom was unquestionably Tomorrowland. To the best of my recollection, I liked Tomorrowland for pretty much the same reasons that Walt was once said to have liked it:

> Tomorrow can be a wonderful age. Our scientists today are opening the doors of the Space Age to achievements that will benefit our children and generations to come. The Tomorrowland attractions have been designed to give you an opportunity to participate in adventures that are a living blueprint of our future.[94]

Tomorowland was Walt Disney's utopia. My favorite of its many attractions was a go-cart ride cleverly named, "Autopia." Although it is difficult now to imagine, Autopia was initially constructed in 1955 during the early days of the developing freeway system in the United States. With little kids riding wee go-carts along miniature cloverleafs, overpasses and multilane straight-aways, Autopia was a hit from the beginning. It represented a time when the concept of free-flowing, limited-access highways remained an unrealized vision.[95] It was Walt's conception of the ideal high-

---

94 Kim Bellotto, Niki Mcneil & Katie Kubush, *In the Hands of a Child: Custom Designed Project Pack -- Disneyland* (Coloma, MI: Hands of a Child, 2007) at 13. See generally Gordon Morris Bakken, *Icons of the American West: From Cowgirls to Silicon Valley* (Santa Barbara: Greenwood Press, 2008).

95 Citizens were fascinated by the abiding dream of the consummate transportation system. At that time, in July 1955, the Santa Ana Freeway was new and legislation to finance the American interstate highway system was still months away from being signed by President Dwight Eisenhower. See Phil Patton, "In Disney's World, a Per-

way — one where the automobile as the icon of personal freedom now survives as a theme park diversion, defying, as one author put it, "the reality of the smog-generating traffic just outside the gates."[96] Autopia remains a testament to the enduring quality of this dream; it is the only ride in all of Disneyland that remains today from the original 1955 plan of the park.

But, to those little kids, Autopia was something else. It was an enormous and amazing ride that wide-eyed seven-year-olds were permitted to go on by themselves, unaccompanied by an adult. This was made possible by virtue of the fact that the go-carts were secured by a railing affixed to the roadway. Although the child could speed up or slow down a little bit, the cart would automatically steer itself along the seemingly endless highway, banking on corners and holding steady down the straight-aways. With the usual magic of Disney, the technological infrastructure that made this possible went completely unnoticed by the kids on the ride; they believed that they were actually driving! Through the illusion of technology, Walt had figured out how to build the literal instantiation of Thoreau's famous observation that, "we do not ride on the railroad; it rides upon us."[97]

I suggest that Disney's Autopia is a much richer conceptual model for understanding the risks posed by digital locks than copy-protected DVDs or e-book readers. Rendered invisible, Autopia's various technological constraints offer the appearance of freedom while in reality disabling the capacity to act through the design of the architecture.[98] Kids can assume the driver's seat, veering a little left or right of centre, but the hidden rail always guides them back into the middle. Unlike training wheels on a bicycle, Autopia's technological infrastructure does not train kids to learn how to drive. In fact it *un-trains* them. Although I had no idea of this as a seven year-old sitting behind the wheel, Autopia's carts are impossible to crash. What I realized, years later, is that Autopia has passengers, not drivers. On Walt Disney's highway, *mistakes are not permitted.*

---

fect Freeway" *The New York Times* (22 August 2005), www.nytimes.com/2005/08/22/automobiles/22CARS.html.

96 *Ibid.*

97 Henry David Thoreau, *The Annotated Walden: Walden; or, Life in the Woods, and Civil Disobedience*, ed. by Philip Van Doren Stern (New York: Clarkson N. Potter, 1970) at 223.

98 As Mark Weiser famously remarked upon coining the term 'ubiquitous computing in 1991': "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." Mark Weiser, "The Computer for the 21st Century," Scientific American 94, (September 1991) http://wiki.daimi.au.dk/pca/_files/weiser-orig.pdf.

Then again, neither is good driving. Autopia automates essential aspects of the driving experience so as to ensure desirable outcomes for the property owner. In other words, *no* driving is permitted. Just like copyright's digital locks, the answer to the machine is, once again, in the machine[99] — which means that it is the property owner who, once again, sits in the driver's seat. All permissions — whether the rider may go north or south, turn east or west — are pre-programmed by the owner of the machine, automated to ensure no possible wrongdoing.

Autopia can be understood as a metaphor for my concern about a generalized digital lock strategy and the automation of permissions. I am concerned about a widespread use of technological constraints — whether in private or public spaces, whether owned or operated by a corporation, a government or an individual — imposed on citizens by property owners who seek total command of their environments. I am concerned because those environments are also our environments. These spaces are crucial to our well-being. They are the playgrounds of our moral development. Yet, digital locks and related techniques allow property owners to eliminate the possibility for moral deliberation about certain kinds of action otherwise possible in these spaces by disabling the world in a way that morally disables the people who populate it.[100] Not by restricting their choices but by automating them — by creating world-altering contrivances that remove people from the realm of moral action altogether, thereby impairing their future moral development.

Consider a second carting example that I experienced some thirty years later. There I was, shopping for groceries at my local Loblaws store, part of Canada's largest food distributer.[101] The lot at the strip mall was rather busy that day, so I ended up parking further down, in front of another box store called Michael's Crafts.[102] While trundling a rather large haul

---

99 Charles Clark, "The Answer to the Machine is in the Machine" in P. Bernt Hugenholtz, ed., *The Future of Copyright in a Digital Environment* (The Hague: Kluwer Law International, 1996) 139. See also Andrew A. Adams & Ian Brown, "Keep Looking: The Answer to the Machine is Elsewhere" (2009) 19 Computers & L. 32; Niklas Lundblad, "Is the Answer to the Machine Really in the Machine?" *Proceedings of the IFIP Conference on Towards The Knowledge Society: E-Commerce, E-Business, E-Government* (Deventer, The Netherlands: Kluwer, B.V., 2002) 733, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.5735&rep=rep1&type=pdf.

100 As I argue below, a widespread digital lock strategy results in something I call "moral disability."

101 Loblaw Companies Limited, "ABOUT US: Company Profile" (2001), www.loblaw.com/en/abt_corprof.html.

102 Michaels (2010) www.michaels.com.

of groceries back to my car one winter's morning, my shopping cart came to a grunting halt. At first I thought it was caused by snow or a piece of ice stuck in the wheel. But when I investigated, I discovered the cart was *intentionally disabled*. One of its wheels contained a locking mechanism that had been triggered by an infrared sensor device detecting that my cart had crossed the store's property line.[103] In order to prevent shopping cart theft and to avoid paying employees to retrieve carts from the four corners of the vast suburban strip mall complex, Loblaws had installed digital locks on their carts to automate the permissions concerning their use. It turns out that my permission to use the Loblaws cart stopped precisely where the property line for Michael's Crafts began. Unfortunately for me, my car was parked a few hundred metres beyond that. There was no one from whom to seek further permission and no one to re-activate the cart. I had to leave the cart on the Loblaws' property, schlep whatever I could carry, and hope that no one stole the rest of the groceries before I could return for a second load.

While novel at the time, this is by now a wholly unremarkable event: something that happens thousands of times a day, everyday, at parking lots across Canada and the US. Except that, the day it happened to me was about one week after Hurricane Katrina rocked New Orleans. Alongside the usual depictions of devastation and ruin, I noticed significant media attention being paid to the imagery of shopping carts, thousands upon thousands of which littered the parking lot and the interior of the New Orleans Convention Center. This should not be surprising. Ever since 1937, when Sylvan Goldman first invented shopping cart technologies as a way to entice people to buy more than they could otherwise carry,[104] uses of the shopping cart have expanded beyond the archetypical shopping experience. Some uses are legal, others illegal. Some are tolerated, others less so. "They have been used as barbecue pits, go-carts, laundry trolleys and shelters. They wind up mostly in apartment complexes, low-income housing and bus stops. Or anywhere else where the person doing the grocery shopping is unlikely to own a car."[105] According to the Food Marketing

---

103 To learn more about what this looks like, see: Carrtronics LLC, "Carrtronics: Partnering Solutions to Curb Losses and Create Profits" (2009) www.carttronics.com/Resources/TechnologyinAction/tabid/68/Default.aspx.

104 See generally Terry P. Wilson, *The Cart That Changed The World: The Career of Sylvan N. Goldman* (Norman: University of Oklahoma Press, 1978).

105 Kelly Wilkinson, "Wheels of Fortune" *Metroactive News* (3 June 1999), www.metroactive.com/papers/metro/06.03.99/shoppingcarts-9922.html.

Institute in Washington, D.C., global losses total more than $800 million annually.[106]

While digital locks therefore make a lot of sense to grocery retailers,[107] those images of New Orleans gave me considerable pause. Would anyone, including grocery retailers, pass moral judgment on Katrina victims for using those carts as they did? It is difficult to imagine. Especially since the very foundation of our legal and moral institutions are clear that in times of necessity, the institution of property must give way to the preservation of life and other core values.[108] But I was further compelled to imagine: what would have happened had there actually been "effective technological measures"[109] on all shopping carts in New Orleans? What further devastation might have occurred for those thousands of unfortunate people using grocery retailers' property out of necessity if it had been technologically disabled?[110]

Remember that the preemptive nature of digital locks leaves no room for forgiveness. Instead, digital locks simply disable the property so that it does not permit of any uses other than its pre-programmed use — which likely would not have contemplated and/or could not otherwise accommodate the range of uses that necessity so often demands. As pre-programmed, preemptive devices meant to automate permissions, digital locks are not law-abiding. To be sure, they can be programmed to comport

106 *Ibid.*

107 The alternative for those retailers would have been to employ shopping cart bounty hunters to "repo" the carts. See Susan Abram, "City Worker is a Wheel Man: Employee Hunts for Abandoned Grocery Carts" *Daily News of Los Angeles* (14 March 2007), www.thefreelibrary.com/CITY+WORKER+IS+A+WHEEL+MAN+EMPLOYEE+HUNTS+FOR+ABANDONED+GROCERY+CARTS. . .-a0160618096.

108 The principle of necessity generally allows a defendant who commits a private wrong in an effort to protect a person or property from imminent harm to be excused from liability that she would otherwise incur. See, e.g., *Sherrin v. Haggerty* (1953), CarswellOnt 391 (Co. Ct.); *Vincent v. Lake Erie Transp. Co.*, 109 Minn. 456, 124 N.W. 221 (1910). The same general principle applies in criminal law. As stated by Dickson J. in *Perka v. R.*, [1984] 2 S.C.R. 232 at para. 11, "[f]rom earliest times it has been maintained that in some situations the force of circumstances makes it unrealistic and unjust to attach criminal liability to actions which, on their face, violate the law." The defence of necessity articulated in that case, "rests on a realistic assessment of human weakness, recognizing that a liberal and humane criminal law cannot hold people to the strict obedience of laws in emergency situations where normal human instincts, whether of self-preservation or of altruism, overwhelmingly impel disobedience" (*Perka* at para. 33).

109 To use the language of the WIPO Copyright Treaties, above at note 63.

110 Which is something we should perhaps also ask ourselves *every time* we see a homeless person with a shopping cart.

with simple legal rules to some extent.[111] And they can be re-programmed if those simple rules are amended. But, generally, these pre-set permissions are unsophisticated and non-negotiable. Lord Denning MR once remarked on this (though he didn't likely know he was talking about "digital locks") in a case involving an automated parking system that only permitted cars to exit the lot upon payment of a fee:

> The customer pays his money and gets a ticket. He cannot refuse it. He cannot get his money back. He may protest at the machine, even swear at it; but it will remain unmoved.[112]

It is one thing to program a digital lock to accord with the terms of a contract.[113] It is quite another to program digital locks that delicately balance public and private interests — which is precisely what both the necessity principle and, for that matter, the law of copyright would require. In the copyright context, none of the Canadian proposed anti-circumvention rules (i.e., rules that would prohibit breaking a digital lock), including those in Bill C-32, have ever contemplated imposing obligations on property owners requiring them to open digital locks in order to permit access that is appropriate or otherwise authorized by law. At best, the anti-circumvention rules permit self-help remedies (i.e., allowing locks to be hacked) for certain non-infringing purposes[114] or as justified by one of the narrow exemptions set out in the legislation.[115] Of course, breaking

---

111 And, even then, only to the extent that the rules are so clear that legal interpretation is unnecessary. In my experience, this is often not the case.

112 *Thornton v. Shoe Lane Parking Ltd.*, [1971] All E.R. 686 at 689, 2 Q.B. 163.

113 Which is the entire purpose of DRM.

114 Shockingly, Bill C-32 does not tie circumvention to an infringing purpose. These new anti-circumvention rules would therefore make it illegal to break a digital lock even in situations where no copyright violation ever occurred. As such, these rules have sometimes been referred to as "paracopyright." See Peter Jaszi, "Intellectual Property Legislative Update: Copyright, Paracopyright, and Pseudo-Copyright" (May 1998), www.arl.org/resources/pubs/mmproceedings/132mmjaszi. See also Ian Kerr, "To Observe and Protect? How Digital Rights Management Systems Threaten Privacy and What Policy Makers Should Do About It," in Peter Yu, ed., *Intellectual Property and Information Wealth: Copyright and Related Rights*, vol. 1 (Westport: Praeger Publishers, 2007).

115 Bill C-32 permits limited circumvention of TPMs for specific purposes: investigations related to the enforcement of laws; activities related to law enforcement and the protection of national security; making computer programs interoperable; encryption research; protection of personal information; access for persons with perceptual disabilities; broadcasting, or telecommunications service on a radio apparatus; and unlocking mobile devices. These provisions, created in s. 47 of the

the lock yourself requires resources and know-how. One can only imagine the further tragedies that would have been reported had Katrina victims been left to their own devices, trying against all odds to re-activate all of those disabled carts.

Consider now a third carting example that I experienced more recently, this time on the golf course. Although I have driven power carts since my dad first showed me how when I was around the age of twelve, I recently experienced "smart carts" while playing for the first time ever on a high-tech golf course. Global positioning systems[116] (GPS) is the key technology, allowing golfers to determine the distance between golf ball and green, understand the layout of the course, track the location of their golf balls and chart their progress on a real-time map. They can also track the play of others, contact the snack cart for a beer or hot dog delivery and satisfy a host of other consumer desires. GPS also allows the club's marshal to know exactly where all players are on the course and how fast or slow they are playing, ensuring an optimal pace of play. The same applications are used by the head greens keeper to monitor employees and valuable golf course assets such as trucks, cars generators, trailers, mowers, sprinklers and the like.[117]

What I learned that day was that smart carts also had digital locks. After a nice approach shot on the second hole, I was driving my cart toward the green when, all of a sudden, the cart was disabled. I had been driving the cart at a decent clip and it just shut right down. And yet, although it would no longer proceed in the forward direction, I was permitted to reverse the cart away from the green and then it turn in any other direction. I later learned that the cart had been deactivated by a GPS tracking system that used geo-fencing technology[118] to immobilize carts that threatened to encroach upon the greens or course boundaries.[119]

While this may seem (virtually) identical to the shopping cart example just offered there is at least one important difference. Unlike shopping

---

amendment, would become ss. 41.11–41.18 in the existing *Canada Copyright Act*. See Bill C-32, above note 10 at cl. 47 [*Anti-Circ*].

116 See generally Ahmed El-Rabbany, *Introduction to GPS: The Global Positioning System,* 2nd ed., (Norwood: Artech House Inc., 2006). See also, Nel Samama, *Global Positioning Technologies and Performance* (Hoboken, NJ: John Wiley & Sons Inc. 2008).

117 For a more detailed descriptions of these features see RavTrack Complete Real-Time Tracking "Golf Course GPS Solutions" 2010, http://ravtrack.com/Golf-Courses.html [Ravtrack].

118 Wikipedia, "Geo-Fence," http://en.wikipedia.org/wiki/Geofence.

119 *Ravtrack*, above note 117.

cart theft, driving toward the green of a golf course or too close to its boundary line is *not* illegal. So it took a while before I grasped the full significance of what had just happened. And, here is how I would describe it. During my previous thirty years of spotty play, golf was regulated by a quaint set of communal norms instilled in newer golfers by those who had truly come to understand and accept the game. "Golf etiquette" was the social instrument for ensuring safety, maintaining the condition of the course, improving the quality of play and showing care and consideration for other players.[120]

To me, etiquette is something to be taken seriously by those who golf. The rules aren't easily learned and their mastery requires significant trial and error. But there is much to be gained from learning how to behave on a golf course. Among other things, it makes one a member of the community of those who play by the rules. Not those who merely conform to the rules but rather those who follow them because they understand their importance and the reasons why those rules were put into place. This requires adopting what Oxford jurist H.L.A. Hart once called "an internal point of view" of the rules. [121] Those who adopt an internal point of view of golf etiquette see themselves as governed by its rules and accept those rules as the reasons guiding their behaviour on the golf course.

This is precisely what was *not* taking place at the high-tech golf course. There, GPS-enabled digital locks automated an array of permissions that included not only when I could buy hot dogs and beer, where I was permitted to drive and how fast, but also whether I was permitted to breach the rule of etiquette about driving power carts too close to the green — one of a series of rules about taking proper care of the golf course. By disabling my ability to drive too close to the green, the property owners were attempting to automate golf's social norms. Just like at Disneyland, I was once again being prevented from making mistakes. No longer would I have to pay careful attention to the rules of etiquette or thoughtfully weigh my actions against what I perceived as appropriate behaviour in light of a particular standard of conduct. Technology took care of all of this by proxy. To the property owners utilizing these machines, I was no longer a golfer; I was no longer a person being called upon to make right or wrong decisions about the appropriate standards of conduct on the golf course.

---

120 See generally Barbara Puett & Jim Apfelbaum, *Golf Etiquette* (New York: St. Martin's Press, 2003).

121 H.L.A. Hart, *The Concept of Law* (Oxford: Oxford University Press, 1961) at 99.

I had become an autonomic extension of the golf machine, robotized by technology in order to ensure optimal efficiency on the golf course.

Consider, finally, a fourth carting example that I have yet to experience, though I may have the opportunity to do so at the end of my driving career. I say this not because the technology I am about to mention is thought to be such a long way off. I say that it will happen at the end of my driving career because the technology I am referring to is called the "driverless car."[122] While this sounds like pure science fiction — didn't George Jetson have one of these? — it is quickly becoming science fact. General Motors' VP of Research and Development, Larry Burns, claims "GM will begin testing driverless cars by 2015 and have them on the road by 2018."[123]

DARPA, the research agency that developed the precursor to the Internet, issued a competition that took place back in 2007 called "the urban challenge."

> This event required teams to build an autonomous vehicle capable of driving in traffic, performing complex maneuvers such as merging, passing, parking and negotiating intersections. This event was truly groundbreaking as the first time autonomous vehicles have interacted with both manned and unmanned vehicle traffic in an urban environment.[124]

More recently, in 2010, a team of Italian engineers launched what has been billed as the longest-ever test drive of driverless vehicles — a 13,000 km, three-month road trip from Italy to China:

> Two . . . vehicles, equipped with laser scanners and cameras that work in concert to detect and help avoid obstacles, are to brave the traffic of Moscow, the summer heat of Siberia and the bitter cold of the Gobi desert before the planned arrival in Shanghai at the end of October.[125]

---

122 That is, once this technology is adopted, I am by definition no longer a driver. Walt Disney's Autopia, it seems, was not so far off the mark.

123 Chuck Squatriglia, "GM Says Driverless Cars Could Be on the Road by 2018" *Wired* (7 January 2008), www.wired.com/autopia/2008/01/gm-says-driverl.

124 The winning team, Tartan Racing, was awarded $20 million. See DARPA, "DARPA Urban Challenge," www.darpa.mil/grandchallenge/index.asp.

125 The Associated Press, "Italy To China In Driverless Vehicles: Italian Team Embarks On 8,000-mile Journey To China Using Driverless Vehicles" *CBS News* (20 July 2010), www.cbsnews.com/stories/2010/07/20/tech/main6694854.shtml.

There are literally hundreds of public and privately funded research consortiums seeking to contribute the future of carting. Projects have included: the US Deptartment of Transportation's "National Automated Highway System Consortium" (NAHS)[126] and, more recently, Europe's Intelligent Speed Adaption (ISA) — "a collective name for systems in which the speed of a vehicle is permanently monitored within a certain area. When the vehicle exceeds the speed limit, the speed is automatically adjusted."[127] ISA experiments have expanded to include broad European participation from countries including: Sweden, the Netherlands, Belgium, Denmark, Britain, Finland, Germany, France, Hungary and Spain.[128] "The standard system uses an in-vehicle digital road map onto which speed limits have been coded, combined with a positioning system."[129] Not unlike the smart golf carts discussed above, one variant of ISA research contemplates a GPS enabled system that "intervenes directly with the fuel supply. As a result it is impossible to exceed the speed limit."[130]

From ox-carts to go-carts, shopping carts, and golf carts, to the driverless carts of tomorrow's Tomorrowland, we see that the potential for corporations, governments, and individuals to control behaviour by placing digital locks and related technological constraints on the devices we have so deeply come to rely upon in daily life is increasing in exponential fashion. This control now extends well beyond the electronic consumer goods that are of interest to the copyright industries. Indeed, one could easily offer detailed accounts along the lines of my carting example across numerous unexpected domains. To mention just a couple, there has been interesting scholarly work[131] applying the digital lock concept to agricul-

---

126 National Automated Highway System Consortium, www.path.berkeley.edu/nahsc/pdf/NAHSC-Presentation_Docs.pdf; see also Richard Bishop, "Whatever Happened to Automated Highway Systems (AHS)?," *Traffic Technology International* (August–September 2001), http://faculty.washington.edu/jbs/itrans/bishopahs.htm.

127 The Netherlands, Ministry of Transport Transport Research Centre (AVV), "Intelligent Speed Adaptation (ISA): A Successful Test in the Netherlands" by Alex van Loon & Lies Duynstee, www.fatedu/~fdimc/laboratorijske_vaje/Inteligentni_transportni_sistemi/Teme_za_studente/Loon%20et%20al%20Intelligent%20Speed%20Adaptation.pdf at 2.

128 European Commission, "Intelligent Speed Adaptation," http://ec.europa.eu/transport/road_safety/specialist/knowledge/speed/new_technologies_new_opportunities/intelligent_speed_adaptation_isa.htm.

129 ISA-UK, "Project Summary" at 1, www.its.leeds.ac.uk/projects/isa/in_depth/project_summary2.pdf.

130 van Loon and Duynstee, above note 127 at 2.

131 Dan L. Burk, "DNA Rules: Legal and Conceptual Implications of Biological 'Lock-Out" Systems" (2004) 92 Cal. L. Rev. 1, http://papers.ssrn.com/sol3/papers.cfm?abstract_

tural biology, wherein "terminator seeds" have been used in "genetic use restriction technologies" to purposely cause second-generation seeds to be sterile.[132] Some of my own ongoing research investigates the use of digital locks in human biotechnology, including human-implantable devices such as RFID chips being used to monitor and maintain biological function,[133] and cochlear implants, which now use digital locks to offer a menu of sound filters and hearing choices for hearing-impaired customer/patients.[134] A stunning array of new examples will emerge with increasing interest in artificial organs and, more generally, the merger of humans and machine systems.

The future is but a question mark. Although the looming uses and limits of digital locks across these broad domains remain uncertain, the examples in this section are meant to provoke and inspire deeper thinking about the potential ethical and legal implications of unimpeded and universal adoption of digital locks. Especially given the strategy of preemption adopted by the powerful entities that currently deploy them.

How might all of this affect us as moral actors who desire to do good things?

E. THE AUTOMATION OF VIRTUE

The question mark that punctuates the end of the previous section is meant as an important point of departure from the existing literature on digital locks and their social implications. As Professors Dan Burk and Tarleton Gillespie have correctly noted, "[t]o date the public debate over deployment of DRM, has been almost entirely dominated by utilitarian

---

id=692061; Jeremy DeBeer "Reconciling Property Rights In Plants" (2005) 8 The Journal of World Intellectual Property 5, http://onlinelibrary.wiley.com/doi/10.1111/j.1747-1796.2005.tb00235.x/abstract.

132 Thus ensuring Bill Gates' famous "planned obsolescence" business model not only in our electronic consumer goods but now, also, for agricultural products used for human sustenance, see generally, Giles Slade, *Made to Break: technology and obsolescence in America* (Cambridge: Harvard University Press, 2006).

133 Ian Kerr, "Chapter 19: The Internet of People? Reflections on the Future Regulation of Human-Implantable Radio Frequency Identification" in Ian Kerr, Valerie Steeves, & Carole Lucock, eds., *Lessons From The Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, 2009), www.idtrail.org/content/view/799.

134 Ian Kerr, "The Components of Health," www.iankerr.ca/publications-mainmenu-70/press-mainmenu-76/762-the-components-of-health.html.

arguments regarding the social costs and benefits of this technology."[135] Indeed, so far as I know, there is only one published article in the entire literature on digital locks that focuses on autonomy and morality and its authors are Burk and Gillespie. Examining "the moral propriety of laws endorsing and encouraging the deployment of DRM,"[136] their excellent article offers a deontological analysis focusing on the moral autonomy of information users.

Like these notable scholars, I am interested in the moral repercussions of what they call a "state sanctioned deployment of DRM."[137] However, the focus of my inquiry is neither utilitarian nor deontological in nature. I want to know how a state sanctioned, generalized deployment of digital locks (i.e., deployment beyond the copyright sphere) might affect us as moral actors. To this end, I turn instead to the third strand in the holy trinity of ethical theory: virtue ethics.

Ever since Elizabeth Anscombe penned her "complaint"[138] about modern moral philosophy in 1958, there has been renewed academic interest in the study of virtue ethics. Disenchanted by modern moral philosophy's fixation with legalistic accounts of ethics and its reliance on utilitarian and deontological conceptions of rights and duties — Anscombe thought that these things generate an unrealistic and absolutist moral oughtism that is rigid and meaningless in a secular society — she pushed for a revitalization of Greek ethics and its questions about the nature of the good life. Like Anscombe, I am interested in these questions. In particular, I wish to consider whether — or how — moral character, virtue and human flourishing might be affected by a state sanctioned, widespread deployment of digital locks.

Although, to my knowledge, it has never previously been characterized in this way, a layperson might reasonably describe the digital lock strategy as an attempt to promulgate the "automation of virtue." Something like this seems already to be a popular sentiment as is evident in this varia-

---

135 Dan L. Burk & Tarleton L. Gillespie, "Autonomy and Morality in DRM and Anti-Circumvention Law" (2006) 4:2 Triple C: Cognition, Communication, Cooperation 239, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1146448 at 239.

136 *Ibid.*

137 *Ibid.*

138 Anscombe was correct in characterizing her own work in its final sentence as a "complaint." Consider, for example, the last line in her opening paragraph where she states her third thesis, namely: "that the differences between the well-known English writers on moral philosophy from Sidgwick to the present day are of little importance." G.E.M. Anscombe, "Modern Moral Philosophy" (1958) 33 Philosophy at 1, www.philosophy.uncc.edu/mleldrid/cmt/mmp.html.

tion on the Yiddish proverb cited earlier — "a lock keeps an honest man honest."[139]

If something like this is the goal of the digital lock strategy, then my professional prognosis for its success is: negatory. This is because the very notion of automating virtue is an oxymoron. The preemption of wrongdoing does not a virtuous person make. A basic account of Aristotle's virtue ethics illustrates not only why this is so but also lays the groundwork for demonstrating what is at stake in the attempt to carry out preemption of this sort. In this section, I will argue that a successful, state sanctioned, generalized deployment of digital locks actually impedes the development of moral character by impairing people's ability to develop virtuous dispositions, thereby diminishing our well-being and ultimately undermining human flourishing. It creates something that I shall call a "moral disability."

Virtue, in the Greek sense, stems from the word *arête*, which is perhaps best understood as "excellence." For Aristotle, the achievement of excellences (there are many) is key to human flourishing. Well-being (*eudaimonia*) is something he understood in terms of the unique function of human beings.[140] What sets humans apart from other animals is the possession of reason. So the proper function of human beings is "activity of the soul in accordance with reason."[141] But to be a person of good moral character, one must not simply act in accordance with reason, one must "perform . . . well and finely, and each thing is completed well when it possesses its proper excellence."[142] Thus, "the human good turns out to be activity of soul in accordance with excellence."[143]

---

139 Wolfgang Mieder, Stewart A. Kingsbury, & Kelsie B. Harder, *A Dictionary of American Proverbs* (Oxford: Oxford University Press, 1992). Copyright owners have taken hold of this particular proverb, equating placing a lock on digital content with simply removing the temptation to break the law. In their paper, "Keep Looking, The Answer to the Machine is Elsewhere," Adams and Brown use the example of a 2003 Congressional committee, in which the Motion Picture Association of America described TPMs as "designed to keep honest users honest." Princeton University encryption expert Ed Felten quipped in response: 'Nothing needs to be done to keep honest people honest, just as nothing needs to be done to keep tall people tall." See Adams and Brown, above note 12 at 2.

140 Aristotle, *Nicomachean Ethics*, trans. by Sarah Broadie & Christopher Rowe (Oxford: Oxford University Press, 2002) at 1097b20-25. Note: all subsequent references to Aristotle's *Nicomachean Ethics* will be cited in the classical style, denoted as *Nic. Ethics* followed by the pinpoint (Bekker number).

141 *Nic. Ethics* 1098a5.

142 *Nic. Ethics* 1098a10-15.

143 *Nic. Ethics* 1098a15.

With this we see that each achievement of virtue is an activity. Well-being "consists in the exercise (not the mere possession of) the virtues."[144] That said, the virtuous character consists in a set of dispositions (*hexeis*)[145] deeply entrenched in the psyche. In good Aristotelian fashion, the development of virtuous dispositions requires both knowing and doing. Most famously, the acquisition of a virtuous disposition requires knowing how and then hitting the right mark (the 'golden mean'):

> excellence of character is an intermediate state . . . it is intermediate between two bad states, one relating to excess and the other to deficiency; and that it is such because it is effective at hitting upon the intermediate in affections and in actions[146]

However, it is important to understand that a virtuous act is not determined by its outcome alone. It also depends upon certain facts about the person performing the act. As Professor David Matheson has characterized it, "[t]he particular kind of dispositions of which the virtues consist is brought about by a consideration of their connection to praiseworthy behaviour, which entails not merely doing the right thing but doing it in the right way."[147] Aristotle sets out three conditions for this, stating that a person's actions are virtuous,

> first, if he does them knowingly, secondly if he decides to do them, and decides to do them for themselves, and thirdly if he does them from a firm and unchanging disposition.[148]

As such, "[c]haracter virtue . . . turns out on Aristotle's account to be deep-seated psychological dispositions to do the right thing (in the relevant context), based on a desire to do the right thing because it is known to be, i.e. recognized as, such."[149]

How, then, is all of this achieved? According to Aristotle, the ability to develop virtuous dispositions to do the right thing based in the desire to

---

144 Roger Crisp, "Virtue Ethics" in Roger Crisp and Michael Slote, eds., *Virtue Ethics* (Oxford: Oxford University Press, 1997) at 2, www.hrstud.hr/hrvatskistudiji/skripte/filozofija/tbracanovic/Etika1/Crisp-Virtue-Ethics.pdf.

145 Virtue is seen as a tendency or disposition, induced by our habits, to have appropriate feelings. See *Nic. Ethics* 1105b25-6.

146 *Nic. Ethics* 1109a20-24.

147 David Matheson, "Virtue and the Surveillance Society" (2007) 3 International Journal Technology, Knowledge, & Society 133 at 135.

148 *Nic. Ethics* 1105a22-b12.

149 Matheson, above note 147 at 135.

do the right things *knowingly* requires, as a necessary precondition, the cultivation of practical wisdom (*phronesis*).[150] *Phronesis* is a special kind of skill, which requires not only an ability to decide how to achieve a certain end, but also the ability to reflect upon and determine that end. As Professor Roger Crisp has noted, *phronesis* is the skillful acquisition of "sensitivity to morally salient features of particular situations which goes beyond an ability to apply explicit rules."[151] Practical wisdom is therefore not something easily acquired and is the reason Aristotle insisted that one must be of a certain age before one can undertake the study of ethics and the development of virtuous dispositions.

> Whereas young people become accomplished in geometry and mathematics, and wise within these limits, young people [endowed with practical wisdom] do not seem to be found. The reason is that *phronesis* is concerned with particulars as well as universals, and particulars become known from experience, but a young person lacks experience, since some length of time is needed to produce it.[152]

Thus the moral attainment of virtue relies fundamentally on practicing, or developing, the virtues in real situations over the course of a lifetime. For, as Aristotle says, "the way we learn the things we should do, knowing how to do them, is by doing them. . .We become just by doing just things, moderate by doing moderate things, and courageous by doing courageous things."[153] Grounded in practice, ethical decision-making of this sort insists that each situation be approached as unique, and considered in its completeness. When the virtuous person finds herself in a difficult situation, she will use all relevant knowledge of the virtues (and of human activity in general), according to the salient moral facts of the circumstances as a guide in making her ethical decision.

With even this rudimentary version of Aristotle's model for understanding and acquiring character-virtue, it is not difficult to see how a universal digital lock strategy would undermine the project of achieving moral excellence.

Honesty, for example, is an intermediary state between an excess and a defect, between exaggeration and fraudulence. To fall short of the mark of honesty is to be dishonest; to exceed it is to be tactless. Among other

---

150 *Nic. Ethics* 1144b14-17.

151 Crisp, above note 144 at 6.

152 *Nic. Ethics* 1142a.

153 *Nic. Ethics* 1103a30-31.

things, honesty involves keeping one's promises. In a legal context, this might sometimes mean honouring the terms and conditions of a contract or licensing agreement. As we have seen, DRM is a souped-up contract — i.e., the terms of its licence can be enforced through the operations of digital locks rather than ethical norms. For instance, if the terms of the license accompanying my e-book are such that I undertake to print no more than ten pages of any books that I download from the service, what this really means, practically speaking, is that the device simply will not permit the printing of an eleventh page.[154]

The e-book reader's lock "keeps an honest person honest" only insofar as someone like me, who has neither the inclination or know-how needed to circumvent it, will probably print ten pages or less. No breach of contract, no broken promises. And, yet, there is *nothing* approaching virtue in my conduct. Recall Aristotle's three conditions for virtuous action set out above. First, it requires being honest knowingly. But, I did *not* knowingly keep my promise. To the extent that the promise was unbroken (since it makes no sense to speak of it in this case as fulfilled), this was not because I knowingly omitted to print an excessive number of pages (heck, I probably didn't even read the terms and conditions of the license requiring such conduct). It was either a coincidence or a consequence of the operations of the software.

Second, according to Aristotle, it is only a virtuous act if my decision to limit myself to ten pages was made *because* it was the honest thing to do. In such case it may never be clear whether my conduct was virtuous. After all, I could have decided to print more than ten pages and yet this still would have made no difference to the outcome, since the digital lock would have complied with the licensing terms no matter what my intentions were. In any event, I probably did not limit myself to less than ten pages because it would be dishonest but rather because it would have been inconvenient to figure out how to do otherwise.

Third, the mere fact that the number of pages printed comported with the licence was not the result of my firm and unchanging disposition toward honesty in the face of temptation but rather because the e-book's robotic code made me do it. The answer to the machine was, as they say, in the machine. But this cannot in any meaningful way be understood as an automation of virtue. To the contrary, technologically compelling me to comply with the terms and conditions of the licence, if anything, pre-

154 In the spirit of Professor Lawrence Lessig's *Free Culture*, I will first borrow, and then later remix, his example found at page 151. See Lessig, above note 11.

vented me from acting in accordance with virtue, let alone acting from any deep-seated disposition towards honesty. Perhaps, eventually, I will reach a point where I simply do anything that the machine doesn't preempt me from doing. *Domo arigato, Mr. Roboto.*

This last point is critical. A series of ubiquitous locks designed to keep people honest would impair the development of a *hexis*, a deep-seated disposition for honesty. Recall the important role that practical wisdom plays in the cultivation of virtue. Virtuous conduct is impossible without *phronesis* — the ability to untie moral knots, to determine both what is good and how to achieve it. Practical wisdom, remember, is a special skill requiring special sensitivity to morally salient features of particular situations. Practical wisdom cannot be programmed. It cannot be cut and pasted. It requires exposure to an array of moral episodes and adventures — opportunities to explore the intricacies of moral deliberation.

Ironically, a ubiquitous digital lock strategy meant to "keep honest people honest" is a self-defeating goal since it impairs the development of *phronesis*, stunts moral maturity and thereby disables the cultivation of a deep-seated disposition for honesty. Woven into the fabric of everyday life, digital locks would ensure particular outcomes for property owners but would do so at the expense of the moral project of honesty.[155]

The cultivation of honesty, like the cultivation of *phronesis*, is a skill. Here, I am reminded of the image of the child riding Walt Disney's Autopia. Recall that the ride permits children to assume the driver's seat, veering a little left or right of centre, but the hidden rail always guides them back into the middle. Just as this is no way to the way to learn how to drive, let alone how to drive well, it is also not how a moral actor achieves the golden mean. The technological procurement of right conduct is not the attainment of virtue.[156]

Although his focus was on the concept of a permission culture rather than its affect on the good life and the attainment of moral excellence, Professor Lawrence Lessig hints at how digital locks might impair the development of *phronesis* and the cultivation of moral virtue:

> The control comes instead from the code — from the technology within which the e-book "lives." Though the e-book says that these

155 And, I suspect, not *just* honesty. Other moral virtues are also at stake.

156 Professor Matheson adopts a similar position, arguing that a "surveillance society risks undermining the ability of its citizens to develop virtue for the same sorts of reasons that overprotective parenting can impair the character development of children." Matheson, above note 147 at 133.

> are permissions, they are not the sort of "permissions" that most of us deal with. When a teenager gets "permission" to stay out till midnight, she knows (unless she's Cinderella) that she can stay out till 2 A.M., but will suffer a punishment if she's caught. But when the Adobe eBook Reader says I have the permission to make ten copies of the text into the computer's memory, that means that after I've made ten copies, the computer will not make any more. The same with the printing restrictions: After ten pages, the eBook Reader will not print any more pages.[157]

For a moment, let's try to imagine a world where virtue-locks could ensure that the teenager *is* home by midnight. Maybe Cindy's coach doesn't turn into a pumpkin[158] but the evolution of the carting industry spawns the development of her FROG AGV 3.0.[159] Taking the lead from Walt Disney's Tomorrowland, this driverless vehicle, complete, let's imagine, with identification and authentication systems, manages a series of permissions pre-programmed by her over-protective parents, resulting in version 3.0 of the classic line, "I have to go now, my ride is here." Only this time round, a series of technological locks prevent Cindy from doing anything other than coming home.

Though I am uncertain whether this thought experiment is fun, frivolous, or just plain frightening, the intended "moral" of the story is important, and is meant to be taken seriously. Professor Lessig's original example implicitly acknowledges something important in Cindy's moral development that comes with having to learn whether to adhere to the curfew rule. To name only a few, her deliberations (should she have any) might include: (1) an evaluation of the importance of the original curfew rule, (2) whether there are legitimate exceptions to it, (3) whether the likely penalty is worth whatever was to be gained from breaking the rule, and (4) the importance of other moral values in conflict with the curfew rule (e.g., staying late to help a friend in need), etc. Cindy's moral deliberations might be epicurean, Kantian, consequentialist, existentialist, eudaimonic, hedonistic, egoistic, spiritualistic, nihilistic, stoic, or pragmatic but, regardless of which, she will be morally knee-capped if technology is permitted to systematically deny her the ability to act upon those deliberations.

---

157 Lessig, above note 11 at 151.

158 Although I imagine this to be the sort of DRM that Tim Burton might like.

159 AGV is the acronym for "Automated Guided Vehicle" systems, the enabling technology for driverless vehicles. See generally Frog AGV Systems, "Over Frog AGV Systems" (2008) www.frog.nl/About_Frog_AGV_Systems/index.php.

To be clear, the critique here is not about her freedom to do as she pleases. It is about the moral disability that she will suffer from not being able to do so. Reiterating from above, the moral attainment of virtue relies fundamentally on practicing the virtues in real situations over the course of a lifetime. À la Aristotle: "we become honest by doing honest things." If locks of various sorts prevent Cindy from making mistakes, from negotiating with herself about what honesty entails or from deciding what *she* will morally permit *herself* to do, her ability and desire to cultivate practical wisdom and the achievement of moral excellence will be impaired. She will become morally disabled.

F. ALEXANDRIAN SOLUTIONS

On Wednesday, 2 June 2010, in the Montreal office of US video-game software developer Electronic Arts, Heritage Minister, James Moore, and Industry Minister, Tony Clement, announced that the Government of Canada would take its third crack at unraveling the Gordian knot of "balanced copyright."[160] In front of a room filled with puzzlers and lock-makers, Minister Clement drew his sword and, with a single dramatic stroke, proclaimed:

> For those companies that choose to use digital locks as part of their business model, they will have the protection of the law.[161]

To anyone paying attention to copyright reform in Canada over the last decade, it shouldn't take a rocket scientist[162] to realize that the anti-circumvention laws"[163] to which Minister Clement was referring are a kind of legal lock — promised by Bill C-32 to copyright owners to further secure

160 It is an unfortunate coincidence that this phrase has been officially adopted by both the Government of Canada *and* "Balanced Copyright for Canada," an industry-based coalition funded primarily by the Canadian Recording Industry Association: http://balancedcopyrightforcanada.ca.

161 Government of Canada, "Speaking Points — Minister of Industry" *Balanced Copyright* (2 June 2010), www.ic.gc.ca/eic/site/crp-prda.nsf/eng/rp01191.html.

162 Although, at least one did. Marc Garneau, former Canadian astronaut and MP for Westmount-Ville-Marie identified digital locks as "the major issue that stands out in the bill" and went on to say that, "the bill seems to be missing an exception that would allow people to break digital locks if it was for private, non-commercial use, but added that his party will have to study it further." See Peter Nowak, "Copyright bill would ban breaking digital locks" *CBC News: Technology & Science* (3 June 2010), www.cbc.ca/technology/story/2010/06/02/copyright-bill-clement-montreal.html#ixzzowllnKJbl.

163 For details on the anti-circumvention provisions, see *Anti-Circ*, above note 115.

the digital lock strategy that industry stakeholders have been lobbying for. As Minister Moore recently noted at a luncheon on "Intellectual Property, Innovation, Economic Growth, and Jobs" in Toronto:

> Copyright owners told that us that their online and digital business models depend on strong protections for digital locks. And they're right. With Bill C-32, we are proposing protections for digital locks. The Bill gives creators stronger legal tools for protecting technological measures including 'digital locks' and other methods. . .[164]

Indeed it does. With all the brute force of an Alexandrian solution, Bill C-32's approach adds a fourth layer of protection[165] to copyright owners through a series of strongly worded prohibitions against: (1) circumventing TPMs that control access to a work;[166] (2) offering services to the public to circumvent TPMs;[167] and (3) manufacturing, importing, distributing, or selling technologies that can be used to circumvent TPMs.[168]

In my view, there are three fundamental flaws with Bill C-32's Alexandrian solution that, operating in conjunction with one another undermines the very possibility of balanced copyright.

First, Bill C-32's anti-circumvention provisions are not tied to copyright infringement, thereby expanding the law of copyright to include acts that have nothing to do with copying. Second, the few exceptions wherein circumvention is permitted[169] are, by many accounts, deficient in scope. Third, Bill C-32 provides what in this chapter, following Burk and Gillespie, I have been calling an "unimpeded state sanction" of digital locks. The first two flaws have been thoroughly canvassed by others in this book and I will not address them here.[170] Instead, I will focus on the third funda-

---

164 Canadian Heritage, "Minister Moore's Speech at Luncheon on Intellectual Property, Innovation, Economic Growth, and Jobs Toronto, Ontario June 22, 2010," www.pch.gc.ca/pc-ch/minstr/moore/disc-spch/index-eng.cfm?action=doc&DocIDCd=SJM100603.

165 Legal protection begins with the law of copyright and its sanctions against infringement. The second layer of protection, used with increasing frequency, is contract law, where the terms of end user licence agreements (EULAs) are used to override existing copyright limitations. As a third layer of protection, many copyright owners have taken it upon themselves to use digital locks.

166 Bill C-32, above note 10 at cl. 47.

167 *Ibid.*

168 *Ibid.*

169 For details on the anti-circumvention provisions, see *Anti-Circ*, above note 115.

170 My view on the first two flaws has been articulated in *Heritage Report Part I*, above note 65; *Heritage Report Part II*, above note 65; *If Left To Their Own Devices*, above note 65.

mental flaw — which is crucial not only to balanced copyright but also to my concerns about the broader use of digital locks set out in this chapter.

In my co-authored two-part study on digital locks commissioned by Canadian Heritage,[171] I enumerated a few observations crucial to the proper scope of protection for digital locks as well as the broader mandate of balanced copyright and then remarked on their policy implications. One such observation was that

> the exercise of any of the exceptions enumerated . . . is premised on the ability to gain access to the work in question.[172]

Consequently, I went on to suggest that any proposed digital lock provisions must therefore

> include a positive obligation on the copyright holder to ensure that alternative means of obtaining access to a work remain available — a "*copy-duty*" . . .[173]

In other words, those who use digital locks might in certain circumstances be obliged to provide a key or at least open the lock whenever someone else has a right to access or use the thing that has been locked-up.

This point is hardly revolutionary. In the ten years since stating it in my second Canadian Heritage study, it has been adopted in one form or other in various countries around the world. For example, the WIPO Standing Committee on Copyright and Related Rights issued a report in June 2010 describing that national laws in at least nineteen Member States provide mechanisms to make sure that prohibition of circumvention of TPMs does not prevent beneficiaries of copyright limitations and exceptions from exercising them.[174] Norway, for example, has established a Ministerial Board, which is empowered to order rightholders to allow access to protected works. Likewise,

> If the rightholder fails to provide access to protected work, many Member States grant beneficiaries of limitations and exceptions a recourse

---

171 To be fair to Minister Moore, these studies where written nearly 10 years ago, back when he was a very junior Member of Parliament and before he was professionally acquainted with copyright reform.

172 *Heritage Report Part II*, above note 65 at 66.

173 *Ibid.* See also Lessig, *Code*: *Version* 2.0 above note 12 at 190.

174 World Intellectual Property Organization, Standing Committee on Copyright and Related Rights, "Report on the Questionnaire on Limitations and Exceptions," SCCR/20/7, Twentieth Session, Geneva, 21–24 June 2010 at 12 www.wipo.int/meetings/en/doc_details.jsp?doc_id=134432.

> to some form of judicial review (e.g. Ireland), arbitration (e.g. Finland), mediation (e.g. Greece) or administrative proceedings (e.g. Estonia).[175]

Poland goes even further, "limiting the application of TPMs only to acts which are not covered by any exception or limitation."[176] In other words, Poland recognizes that there are uses of digital locks that should be outright prohibited (in a way that mere exemptions will not do). In sum, by limiting or prohibiting the use of some digital locks altogether, or requiring the rightholder to open the lock, these Member States have recognized that an absolutist über-protection of digital locks thwarts the possibility of balanced copyright[177] and creates even greater risks outside of copyright's vast empire.

Ten years and three copyright bills later, the Government of Canada has once again tabled a bill that exclusively provides "strong protections *for* digital locks." For the third time running, it has done so without imposing appropriate balancing counter-measures for circumstances in which some measure of public interest might require strong protection *from* digital locks. Bill C-32 contains no countervailing provisions that would set limits or impose obligations concerning the use of locks, and certainly no provisions that prohibit particular uses of them or require them to be unlocked. *In other words, Bill C-32's legal locks provide a total lock on locks*. Those who have them can use them however they so choose with total impunity.[178]

---

175 *Ibid.*

176 *Ibid.*

177 Thanks to Michael Geist for useful discussions on this point, including reference to the following excellent article: Urs Gasser and Silke Ernst, *EUCD Best Practice Guide: Implementing the EU Copyright Directive in the Digital Age,* University of St. Gallen Law School: Law and Economics Research Paper Series Working Paper No. 2007-01, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952561.

178 In fact, if you read the government's speeches, FAQs and talking points, you will notice the language surrounding digital locks is peppered with soundbytes employing "freedom" and "choice" *for the property owner.* The section of the government's 'Balanced Copyright' website identifying key provisions of Bill C-32 includes this quote: "Businesses that choose to use digital locks as part of their business models will have the protection of the law." See Government of Canada, "What the New *Copyright Modernization Act* says about Digital Locks (8 June 2010), www.ic.gc.ca/eic/site/crp-prda.nsf/eng/rp01189.html. Another part of the website articulates what Bill C-32 will mean for copyright owners, artists and creators. With reference to the digital lock protections required by the WIPO Internet Treaties, the following is stated: "Protecting digital locks gives copyright industries the certainty they need to roll out new products and services, such as online subscription services, software and video games, if they choose to use digital locks. Not only will this promote investment and growth in Canada's digital economy, it will also encourage

The reasons for my broader concerns about this unimpeded, state sanctioned digital lock strategy should by now be clear in light of my analysis in Sections B and C of this chapter. The "permission" that Bill C-32 would give to property owners to make unimpeded use of digital locks is premised on a misconception of the function of locks as mere instruments of exclusion used to protect private property. In its bold Alexandrian reaction to digital copyright's Gordian knot, Bill C-32 fails to acknowledge the fact that locks properly understood are access-control devices premised not only on authorized permission by the copyright owner but, also, *permission authorized by the law*.

The fatal flaw is this: Bill C-32 refuses to recognize that foundational legal rules or principles might sometimes require property owners to open digital locks in order to permit justified access or use. As I stated in my second Canadian Heritage study, this is not merely the passing fancy of wishful academics — or, dare I now say, "radical extremists."[179] It has its basis in Canadian constitutional law, and is already supported in principle in the copyright context by the Supreme Court of Canada in the following passage from *Haig v. Canada:*

> . . . a situation may arise in which, in order to make a fundamental freedom meaningful, a posture of restraint would not be enough, and positive governmental action might be required. This might, for example, take the form of legislative intervention aimed at preventing certain conditions which muzzle expression, or ensuring public access to certain kinds of information.[180]

It is absolutely essential to note that a legal duty requiring property owners to open digital locks in order to permit justified access or use is totally separate and distinct from self-help remedies indirectly available through the exceptions contemplated within the anti-circumvention prohibitions. For example, to say that I have a right to circumvent a lock in

---

the introduction of innovative online services that offer access to content." (21 June 2010) www.ic.gc.ca/eic/site/crp-prda.nsf/eng/rp01189.html.

179 While addressing the International Chamber of Commerce in Toronto on Tuesday, 22 June 2010, Minister Moore advanced the claim that any people opposed to the new legislative provisions prescribed by Bill C-32 belonged to two groups of 'radical extremists'. For news reporting on this event, see Peter Nowak, "Copyright debate turns ugly: Heritage minister stirs hornet's nest with 'radical extremist' comments," *CBC News* (24 June 2010), www.cbc.ca/technology/story/2010/06/23/copyright-heritage-minister-moore.html.

180 *Haig* v. *Canada* [1993] 2 S.C.R 995, http://csc.lexum.umontreal.ca/en/1993/1993scr2-995/1993scr2-995.html at para. 79.

order to protect my personal information pursuant to the exceptions set out in Bill C-32 is *certainly not* the same thing as having a law wherein the state requires a party that collects, uses or discloses information about an identifiable individual to open the lock under circumstances where data protection law would demand it. The same argument could be made in the context of copyright laws where user rights might demand something more than the exception set out in Bill C-32. I further suspect that the principle I am articulating here is of general application. As I tried to make clear in my analysis of digital locks in the case of shopping carts, laws that would authorize, justify or excuse the circumvention of a lock — or, for that matter, impose upon the property owner a duty to open it — will often fall outside of the private ordering rules that are created and controlled in their entirety by property owners. Believe it or not, they could also fall outside of the ambit of law of copyright. ;)

While it is hard to imagine a foundational principle like the law of necessity actually creeping into a copyright infringement case, there are a myriad of legal rules and principles that could do so from both inside and outside of copyright law. The *Haig* case, mentioned above, is one such example. The problem with Bill C-32 is that its bold, unimpeded, absolutist Alexandrian protection of digital locks misunderstands the purpose and function of a lock which, at least in the case of more sophisticated access-control systems, not only hinders unauthorized access but also provides a mechanism for situations where the property owner has not contemplated a need for access but one later arises. The best security systems not only prevent access to interlopers but also grant access to those who have or ought to have permission.

The protection afforded to digital locks in Bill C-32 would, in situations such as the ones we are imagining, allow the property owner to trump the public interest for no other reason than being the *de facto* keyholder. Without a legal mechanism that imposes a duty on a property owner to open or remove the lock when the law would otherwise authorize doing so but the property owner would not, private ordering through the use of digital locks will become the rule and property owners the rule-makers. Balanced copyright doesn't stand a chance.

In witnessing this decade long Sisyphean error, I am tempted to understand the Alexandrian solution[181] offered by Ministers Clement and Moore

181 My use of several historical versions of the Alexandrian myth throughout this chapter is offered as a richer illustration of the difference between brute force and elegant solutions. The methodology of using classical mythology as a framework

not in accordance with the popular version of the legend wherein Alexander the Great is the solver of the knot's puzzle and the hero of the prophesy. Perhaps it seems more in line with a less popular account of the legend. In this alternative version,

> an exasperated Alexander is unsuccessful in every legitimate attempt.
>
> his whole body
> drenched in sweat
> while I
> sat nearby
> quietly
> watching
>
> (Ba. 620-2) — Euripides' Bacchae

---

for understanding contemporary problems is well established. For instance, "[t]wo of our oldest metaphors tell us that all life is a battle and that all life is a journey; whether the *Iliad* and the *Odyssey* drew on this knowledge or whether this knowledge was drawn from the *Iliad* and the *Odyssey* is, in the final count, unimportant, since a book and its readers are both mirrors that reflect one another endlessly." See Alberto Manguel, *Homer's The Iliad and The Odyssey: A Biography* (Vancouver: Douglas & McIntyre, 2007) at 2. James Joyce's *Ulysses* also evokes classic Greek literature. In the despair and unrest that was the shattered modern world post-WWI, Joyce uses the familiar journey of Odysseus to inject a sense of order that will resonate with readers. In a famous review of *Ulysses*, T.S. Eliot makes a similar point: "[i]n using the myth, in manipulating a continuous parallel between contemporaneity and antiquity, Mr. Joyce is pursuing a method which others must pursue after him . . . It is simply a way of controlling, of ordering, of giving a shape and a significance to the immense panorama of futility and anarchy which is contemporary history." See Michael Bell, *Literature, modernism and myth: belief and responsibility in the twentieth century* (Cambridge: Cambridge University Press, 1997) at 122. Joyce calls himself only "a shy guest at the feast of the world's culture," but nonetheless succeeds at characterizing modern life through the veil of antiquity. This technique of using myth to understand modern culture has been seen in countless stories. See Gilbert Highet, *The classical tradition: Greek and Roman influences on western literature* (Oxford: Oxford University Press, 1949) at 518. Another popular mythological figure, Hercules, has "embodied or endorsed" a wide range of ideas or opinions. Such an example has broad cultural appeal, due to the various myths emanating from this fascinating figure. As biographer Alastair Blanchard has written "Biography attempts to make the world understandable. It is our response to chaos." By using these tales as a framework, we are empowered to think critically about our own culture through the eyes of an ancient persona. Alastair Blanchard, *Hercules: A heroic life* (London: Granta Books, 2005) at xix.

> Faced with the specter of conspicuous failure, Alexander slashes the knot in two with his sword.[182]

As one biographer described this outcome, "Alexander was a man incapable of shrugging his shoulders and walking away from an unsuccessful effort. If, as a result of several futile attempts, he was frustrated and angry, he might very well have decided that a sudden stroke of the sword would rescue him from public embarrassment."[183]

However, my goal here is not so much to critique Bill C-32 or its proponents as it is to inspire deeper thinking about the potential ethical and legal implications of an unimpeded and universal adoption of digital locks, especially given the strategy of preemption adopted by the powerful entities that current deploy them. In the spirit of doing so, I offer yet a third account of the legend of the Gordian knot, known mostly by historians and scholars in the field of classical studies.

> [Alexander] saw the celebrated chariot which was fastened to its yoke by the bark of the cornel-tree . . . According to most writers the fastenings were so elaborately intertwined and coiled upon one another that their ends were hidden: in consequence Alexander did not know what to do, and in the end loosened the know by cutting through it with his sword, whereupon the many ends sprang into view. *But according to Aristobulus he unfastened it quite easily by removing the pin which secured the yoke to the pole of the chariot, and then pulling out the yoke itself.*[184]

Like our protagonist in Aristobulus' account, I prefer elegance to brute force. And, yet, elegant solutions are not always the stuff of political expedience. I know that there are many senior government lawyers, policy advisors and bureaucrats working on the digital copyright file who understand these arguments as well — better, actually — than the academics seeking to contribute to their improvement. The flaws in Bill C-32 are symptomatic of the larger digital lock strategy upon which they are modeled. As I have suggested in this chapter, the legal locks, just like the digital locks, just like the mechanical locks, must be understood as something more than instruments of exclusion to be used at the whim of those who hold them in their hands. One must remember that the preemptive nature

---

182 John Maxwell O'Brien, *Alexander the Great: The Invisible Enemy, A biography* (London: Routledge, 1992) at 70–73.

183 *Ibid.*

184 Plutarch, above note 4 at 271 [emphasis added].

of digital locks leave no room for forgiveness. Instead, digital locks simply disable the property so that it does not permit any uses other than its pre-programmed use. Perhaps more significantly, moving to the moral sphere, I have also suggested that a series of ubiquitous locks designed to keep people honest would impair the development of a *hexis*, a deep-seated disposition for honesty, by discouraging or preventing the development of practical wisdom.

My argument in this chapter has been cast through the lens of virtue, the ancient Greek idea that the good life is to be lived through the attainment of moral excellence. From this point of view, practical wisdom cannot be uploaded or downloaded. It requires a broad variety of life experiences — opportunities to navigate the messy, complex world of moral decision-making. It also requires making mistakes. How could we possibly live well, let alone flourish, in environments that increasingly seek to control our behaviour with fine-tuned granularity, by the flick of a switch permitting or forbidding various courses of conduct not proscribed by law but by lock-makers? How are we to cultivate a moral compass, a sense of right and wrong, good and bad, if we are locked on a course that leads us only from here to there with no opportunity for moral journey, deliberation or error? And what, other than some form of robotic habituation, would make us think that those endowed with the power to use digital locks in this way should have a monopoly on right conduct in the first place, or that they are always justified in using the locks as they do?

As Elizabeth Anscombe has noted, the attainment of virtue is foreign to the law's language of rights and duties. Perhaps the unity of these distinct discourses finds expression in the words of the philosopher, Joseph Raz, whose thoughts on the relationship between the morality of freedom and copyright law's concept of authorship are worthy of citation:

> All too often moralists tend to regard a person's moral life as the story of how he proves himself in the face of moral demands imposed on him by chance and circumstance. Crucial as this aspect is, it is but one side of a person's moral history. The other side of the story evolves around the person not as the object of demands imposed from the outside, but as the creator of such demands addressed to himself. We are all to a considerable degree the authors of our moral world.[185]
>
> . . .

185 Joseph Raz, *The Morality of Freedom* (New York: Oxford University Press, 1986) at 86.

> Autonomy requires that self-creation must proceed, in part, through choice among an adequate range of options; that the agent must be aware of his options and of the meaning of his choices; and that he must be independent of coercion and manipulation by others. Personal autonomy is the ideal of free and conscious self-creation.[186]

If we are to remain, to a considerable degree, the *authors* of our *moral world*, we must maintain the ability to access it and make use of it. While the law of copyright affords protection to the creators of original works, a balanced copyright scheme must not, in the process, diminish the very possibility of self-creation. Excessive protection of digital locks places coercive limits on moral actors, preventing them from acquiring access to an adequate range of life's options. What would be the point in developing entire systems to protect creative works or other forms of property if the means by which this is achieved ultimately undermines *moral authorship* and the project of *conscious self-creation*?

186 *Ibid* at 390.