Learning the Hard Way: The Anti-Circumvention Amendments to the Hong Kong Copyright Ordinance

Robert S. Rogoyski*

The 2007 Hong Kong Copyright Amendment Ordinance was passed as part of continuing efforts to balance the interests of copyright owners with the public benefits that flow from the use of copyrighted works. The anticircumvention provisions in the ordinance, closely modeled on the U.S. Digital Millennium Copyright Act (DMCA), create a complex new regime that regulates the circumvention of copy and access controls to copyrighted works, and contains a set of narrow exceptions for some scientific research. Both the specific text of the amendments, and U.S. experience with similar provisions in the DMCA give rise to serious concerns about the potential effects of this legislation. The anticircumvention amendments threaten fair dealing rights in Hong Kong because they unduly expand the power of copyright owners to control the actual use of their works, rendering fair dealing rights moot. Although the amendments provide exceptions for cryptography and security testing, the wording of the exceptions is problematic, and U.S. experience with very similar provisions in the DMCA shows that they will nevertheless chill legitimate research and harm consumers.

* © 2008 Robert S. Rogoyski. J.D. cum laude 2005, Harvard Law School; LL.M. 2008, University of Hong Kong. An earlier version of this Article was submitted in partial satisfaction of graduation requirements at the University of Hong Kong. I would like to thank Kevin Pun and Amanda Barnett for their invaluable opinions and suggestions.

I. INTRODUCTION

It is the express goal of the Administration of the Hong Kong Special Administrative Region (SAR) to "provide Hong Kong with a strong system of copyright protection to facilitate the development of a knowledge-based economy and creative industries."[1] The Administration recognizes, however, that pursuit of this goal must be tempered by careful attention to competing interests.[2] On the one hand, copyright owners demand strong legal protection.[3] On the other hand, an unbalanced copyright regime could disrupt the public benefits that result from the "free-flow and dissemination of information arising from the use of copyright works."[4] It was in this spirit of compromise and concern that the Administration passed a new Copyright Amendment Ordinance, which was gazetted on July 6, 2007.

Among the provisions included in the amendments are anticircumvention provisions that bear a striking similarity to anticircumvention provisions in the U.S. Digital Millennium Copyright Act (DMCA). These provisions greatly expand the existing prohibitions in the Copyright Ordinance (CO) on devices that circumvent copyright technological control measures (TCMs). The new regime creates a complex web of civil and criminal liability relating to circumventing copyright TCMs, as well as a set of liability exceptions.

In this Article, I will argue that the Hong Kong anticircumvention amendments have serious problems that demand attention. As of this writing, these amendments have not yet come into effect. Although the amendments may not be tested in court for some time, the world of copyright is driven by ex ante incentives and out-of-court legal maneuvering. Thus, it is important to recognize issues early on so that Hong Kong may avoid chilling effects now, and potentially harmful judicial interpretations of the amendments in the future.

In Part II, I will argue that the Hong Kong amendments are subject to the same, heavy criticism that numerous scholars have heaped upon

---

1. Report of the Bills Committee on Copyright (Amendment) Bill 2006, p. 1, LC Paper No. CB(1)1844/06-07, June 8th 2007, *available at* http://www.legco.gov.hk/yr06-07/english/hc/papers/hc0608cb1-1844-e.pdf.
2. *See id.* at 2.
3. *Id.* at 1-2.
4. *Id.*

the DMCA: the anticircumvention amendments pose a serious threat to fair dealing rights. In Part III, using a careful textual analysis of the anticircumvention exceptions and drawing on several examples from the U.S. experience with the DMCA, I will argue that the new amendments also endanger legitimate TCM-research and consumer digital security interests in Hong Kong.

II. THE CO ANTICIRCUMVENTION AMENDMENTS POSE A SERIOUS THREAT TO FAIR DEALING RIGHTS IN HONG KONG

A. How Can This Be?

The allegation is serious. Yet, the Bills Committee, specifically, and more generally the Legislative Council were clearly aware of the need to balance the interests of content owners with the fair dealing interests of the general public.[5] So, how is it possible that the anticircumvention amendments seriously threaten fair dealing rights? The answer is simple: by overprotecting the technology, the anticircumvention amendments render the fair dealing provisions in the CO moot.

First, let us consider the CO section 273 of the CO's circumvention provisions, effective since January 2001, which focuses specifically on circumvention devices.[6] These provisions create a civil remedy for the person issuing legitimate copies of a copy-protected work against a person who, knowing the device will be used to infringe copyrights, makes a device that circumvents copy protection, generally "trades in" such a device, possesses such a device in connection with any sort of trade or business, or publishes information to help others circumvent the particular form of copy protection used.[7] Notably, these provisions do not cover the purchase of such a device. And, although there are situations where this device restriction could still cramp fair dealing rights, the requirement of knowledge that the device will be used to infringe copyrights will tend to protect a good-faith user. For example, a teacher using a device to circumvent e-book copy protection in order to quote a paragraph for a class would "possess" the device in the course of a trade (teaching). However, that possession would "knowingly" be for noninfringing purposes only.

---

5. *Id.*

6. Copyright Ordinance (1997), Cap. 528, § 273 (H.K.), *available at* http://www.wipo.int/clea/docs_new/pdf/en/hk/hk001en.pdf.

7. *Id.* § 273 (2)(a).

The new amendments, which repeal and replace the 2001 circumvention provisions,[8] are quite expansive. In addition to substantially augmenting existing restrictions on "devices," the amended section 273A(1) "applies where an effective technological measure has been applied in relation to a copyright work, and a person does *any act* which circumvents the measure, knowing, or having reason to believe, that he is doing an act which circumvents the measure."[9]

"Effective technological measure" is defined in sections 273(2)(a) and (b) as a measure that functions as an "access control or protection process" or "copy control mechanism," respectively.[10] In a case of circumvention, the copyright owner, exclusive licensee, and any other licensee who issues copies, makes the copyright work available, or broadcasts the work can *concurrently* bring a civil lawsuit for copyright remedies against the party engaging in circumvention.[11] The new section 273D also creates a list of seven limited exemptions to section 273A for members of the public:

(1) achieving interoperability of an independently created computer program;
(2) research into cryptography;
(3) identifying and disabling the function of a technological measure to collect or disseminate information which tracks and records the manner of a person's use of a computer network (spyware) in order to protect privacy;
(4) security testing for a computer or computer system/network;
(5) gaining access to parallel imported copies of copyright works;
(6) preventing access by minors to harmful materials on the Internet (screening software); and
(7) copying for preservation and replacement purposes by the librarian or archivist of a specified library or archive under section 50, 51 or 53 of the Copyright Ordinance.[12]

---

8. Copyright (Amendment) Ordinance 2007, Ord. No. 15 of 2007, at A773 (H.K.), *available at* http://www.legco.gov.hk/yr06-07/english/ord/ord015-07-e.pdf.

9. *Id.* at A777.

10. *Id.* at A775.

11. *Id.* at A777.

12. FAQs on Copyright (Amendment) Ordinance 2007, Intellectual Property Department, The Government of the Hong Kong Special Administrative Region Intellectual Property Department, FAQs on Copyright (Amendment) Ordinance 2007, http://www.ipd.gov.hk/eng/intellectual_property/copyright/faq_copyright_protection.pdf (last visited Nov. 18, 2007); *see also* Copyright (Amendment) Ordinance 2007, Ord. No. 15 of 2007, at A785-A791, *available at* http://www.legco.gov.hk/yr06-07/english/ord/ord015-07-e.pdf (last visited Nov 20th, 2007). Section 273D further exempts anticircumvention acts "done by, or on behalf of, law enforcement agencies for the purpose of the prevention, detection or investigation of an offence, or the conduct of a prosecution." Ord. No. 15 of 2007, at A791.

In plain terms, if you circumvent either an access control or a copy control mechanism on a copyright work, and what you are doing does not fall into one of the specified exemptions in amendment 273D, then you can be sued. The wrongful act is the circumvention itself—there is no general exemption for fair dealing.

One might initially argue that there is an exemption for fair dealing under amendment 273(1)(c), which states that "the reference to use of a copyright work does not extend to any use of the work which is outside the scope of the acts restricted by the copyright in the work."[13] However, there are two reasons why this defense is unavailing. First, fair dealing in the CO relates "only to the question of infringement of copyright; it does not affect any other right or obligation restricting the doing of any of the specified acts."[14] In other words, acts of fair dealing are acts which are restricted by copyright, but they are defined as noninfringing acts when they meet certain requirements.

Second, in a FAQ distributed on the Hong Kong Intellectual Property Department's Web site, the government has made its position on the statute very clear: "[Y]ou may attract civil liability if you knowingly circumvent a technological measure, even though your intention is not to commit an infringing act."[15]

And, as will be explained further below, even if there were a limited exemption for fair dealing in the statute, without clear protection fair dealing rights could still be powerfully eroded.

B. How Bad Could It Be? Lessons and Advice from Across the Pond

The amendments to the CO are similar in many respects to the anticircumvention provisions in the DMCA.[16] Thus, even though the amendments have not yet been tested by courts in Hong Kong, it is possible to make predictions about their potential effects on fair dealing in Hong Kong based on the U.S. experience over the last seven years.[17] With this experience as our guide, it is clear that there are significant grounds for concern.

---

13. *See* Ord. No. 15 of 2007, *supra* note 8, at A775.

14. *See* Copyright Ordinance (1997), Cap. 528, § 37(1) (H.K.).

15. FAQs on Copyright (Amendment) Ordinance 2007, *supra* note 12, at 14.

16. Digital Millennium Copyright Act § 1201, Pub. L. No. 105-304, 112 Stat. 2860, 2863-72 (1998).

17. Though the DMCA was passed into law in 1998, the anticircumvention provisions did not come into effect until two years after the date of passage. 17 U.S.C. § 1201(a)(1)(A) (2000).

It must be noted at the outset that, unlike the CO amendments, the DMCA does make a limited exemption for "fair use."[18] Although "fair use" rights are broader than Hong Kong's "fair dealing" rights, for present purposes they can be treated as roughly equivalent. Like the amendments to the CO, as a general matter the DMCA prohibits circumvention of "a technological measure that effectively controls access to" a copyright work.[19] However, this prohibition on the act of circumvention does not "affect rights, remedies, limitations, or defenses to copyright infringement, including fair use."[20] As a result, the DMCA prohibits circumventing an *access* control, but if you legitimately access a copyright work there is no prohibition against circumventing a *copy* control measure to engage in fair use.

During the debates on the DMCA, the U.S. Congress was well aware of both the tension between the interests of content creators and the interests of content users, and the public policy in favor of fair use.[21]

> Fair use, thus, provides the basis for many of the most important day-to-day activities in libraries, as well as in scholarship and education. It also is critical to advancing the personal interests of consumers. Moreover, as many testified before the Committee, it is no less vital to American industries, which lead the world in technological innovation. As more and more industries migrate to electronic commerce, fair use becomes critical to promoting a robust electronic marketplace.[22]

The United States Congress endeavored to address these issues by creating the compromise position described above. To protect the content owners, circumventing access controls became a wrongful act.[23] But, allowing users to circumvent copy controls for noninfringing acts, it was thought, would balance the competing interests and "ensure that the concept of fair use [remained] firmly established in the law."[24]

Despite this attention on the part of the United States Congress to the "vital" importance of fair use rights, the DMCA was criticized at its inception,[25] and has been heavily criticized ever since for the damage it

---

18. *See* Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary, at 4, 1998, *available at* http://www.copyright.gov/legislation/dmca.pdf (last visited Nov 18, 2007).

19. 17 U.S.C. § 1201(a)(1)(A).

20. *Id.* § 1201(c)(1).

21. *See* Digital Millennium Copyright Act Of 1998, WIPO Copyright Treaties Implementation and On-Line Copyright Infringement Liability Limitation, H.R. REP. NO. 105-551, pt. 2, 1998 WL 414916, at *25-26 (1998).

22. *Id.*

23. *See id.*

24. *Id.*

25. *See, e.g.*, Lawrence Lessig, *The Law of The Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 537-38 (1999), *available at* http://lessig.org/content/articles/works/

inflicts on legitimate uses of copyright.[26] As copyright scholar Lawrence Lessig presciently observed the year the DMCA was passed, the core problem is that for copyright purposes, the protection granted by the access control restrictions is overly broad.[27] Even though there is neither intent nor actual infringement of copyright, the access-TCM-circumventing user will still be in violation of a law designed to protect copyright interests.[28] As a practical matter, this changes the relationship between the copyright owner and the user.[29] At the origin of the supply chain, the copyright owners will tend to package TCMs with other "measures." Some of these will be legal, contractual measures—various forms of the End User License Agreement—that will require that users agree to further restrictions of their rights in exchange for access to the copyright work.[30] Access TCMs will also be packaged with copy control TCMs such that they are inextricably interwoven—you cannot crack one without cracking both, and thus violating the law. Therefore, the net effect of the access control protection is to "virtually negate fair use with respect to many works offered in digital media."[31]

---

finalhls.pdf (discussing the DMCA as an example of over-inclusiveness); *see also* Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813, 814 (2001); Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813, 814 (2001) ("Copyright is dead. The [DMCA] has killed it."); Jeff Sharp, *Coming Soon to Pay-Per-View: How the Digital Millennium Copyright Act Enables Digital Content Owners To Circumvent Educational Fair Use*, 40 AM. BUS. L.J. 1, 2 (2002) (stating that the DMCA will have a negative impact on education).

26. *See, e.g.*, *Unintended Consequences: Seven Years Under the DMCA*, Electronic Frontier Foundation, *Unintended Consequences: Seven Years Under the DMCA*, 12 (2006), http://www.eff.org/IP/DMCA/DMCA_unintended_v4.pdf ("Years of experience with the 'anti-circumvention' provisions of the DMCA demonstrate that the statute reaches too far, chilling a wide variety of legitimate activities in ways Congress did not intend."); Timothy B. Lee, Cato Inst., Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act, 9-10 (2007), http://cato.org/pub_display.php?pub_id=6025 (arguing that the DMCA has the practical effect of dramatically broadening the scope of digital copyrights and narrowing the freedom of individuals to use content they have legally purchased); Nicola Lucci, *The Supremacy of Techno-Governance: Privatization of Digital Content and Consumer Protection in the Globalized Information Society*, 15 INT'L J.L. & INFO. TECH. 192, 193 (2007)] (arguing that the DMCA compromises "the consumer's capacity to exercise legitimate rights"); Gideon Parchomovsky & Kevin A Goldman, *Fair Use Harbors*, 93 VA. L. REV. 1483, 1522 (2007) (stating that the harsh criticisms of other commentators are well founded); Michael Landau, *Has the Digital Millennium Copyright Act Really Created a New Exclusive Right of Access?: Attempting To Reach a Balance Between Users' and Content Providers' Rights*, 49 J. COPYRIGHT SOC'Y U.S.A. 277, 293 (2001) ("[T]here are major problems with the anti-circumvention provisions in section 1201.").

27. *See* Lessig, *supra* note 25.

28. *See id.* at 537.

29. *See* Lucci, *supra* note 26, at 220.

30. *See id.*

31. Parchomovsky & Goldman, *supra* note 26, at 1522.

Recent scholarship on the DCMA is overwhelmingly negative. The DMCA "anticircumvention provisions have been used to stifle a wide array of legitimate activities, rather than to stop copyright infringement," and the DMCA has "developed into a serious threat to several important public policy priorities."[32] It has reduced consumer choice, and has been used to block market competition, research, and public criticism.[33] It has also been hailed as an "inappropriate delegation of governmental decision making to a non-governmental entity" leading to serious threats to "freedom of expression as well as privacy."[34]

C. Implications for Hong Kong

All the same criticisms listed above are applicable to the anticircumvention amendments to the CO. In fact, the situation will be worse in Hong Kong because there is no general exception for fair use/fair dealing, and, unlike the DMCA, circumventing both access *and* copy control TCMs is prohibited in the amendments. In turn, Hong Kong faces the same list of harms.

In defense of the Hong Kong anticircumvention amendments, one can cite the results of a recent, major U.S. study on fair use in the United States. The study, commissioned by the Computer and Communications Industry Association (CCIA), found that economic activity based on fair use exceptions was responsible for more than $4.5 trillion in annual revenue in the U.S.—one-sixth of total U.S. GDP.[35] Moreover, this revenue represented a thirty-one percent increase over 2002 levels.[36] This seems to grate with the DMCA lamentations of the legal scholars. If the DMCA is so bad for the United States, how is it possible for fair use to be such a huge part of the U.S. economy? Does Hong Kong really have so much to fear from this example?

The answer is that the "fair use-age" continues in the United States in spite of the DMCA. First, though there are few examples of litigation that focus purely on fair use (as opposed the multitude of cases that combine the issue with other harmful anticircumvention provisions discussed in Part III, *infra*), the gauntlet has been thrown down. The CCIA—which includes technology industry heavyweights such as

---

32. Electronic Frontier Foundation, *supra* note 26.

33. Lee, *supra* note 26, at 9-10, 19.

34. Lucci, *supra* note 26, at 192, 213.

35. Thomas Rogers & Andrew Szamosszegi, Computer & Commc'n Indus. Assoc., Fair Use in the U.S. Economy: Economic Contribution of Industries Relying on Fair Use, 9 (2007), http://www.ccianet.org/artmanager/uploads/1/FairUseStudy-Sep12.pdf.

36. *Id.* at 7.

Microsoft, Google, and Yahoo—launched a web site called Defend Fair Use.[37] The Web site "calls on the [U.S.] Federal Trade Commission to crack down on media companies' copyright infringement lawsuits";[38] it also encourages individual web users to sign petitions and make statements in favor of fair use.[39] Although this battle extends beyond the specifics of the DMCA, it demonstrates the extent to which even major players in the United States are rising up against the current copyright regime.

Second, the technology is still relatively new. The digital environment itself has hardly been around for very long, so the digital technologies for protecting copyright are nascent. Moreover, we do not yet live in an entirely digital world. But, the trend over recent years has become clear. Physical media are being phased out—and digital downloads and content streaming are phasing in. Libraries around the world are digitizing their collections, and a substantial percentage of all basic research in industrialized countries occurs over a network. Hong Kong is one of the most well-wired regions in the world. As the digital revolution progresses, more and more works entering and being produced in Hong Kong will be protected by some form of TCM.

Third, it is hard to measure the true extent of the damage from stifling fair use or fair dealing because the victims are often invisible. Many times we can only speculate because the issue is what would have happened, but did not, because of a "chilling effect" caused by fear of litigation. One might interject here that circumvention activities by individuals might only take a dent out of fair use. A large percentage of the population will be unaware of the anticircumvention laws, and many simply will not care because they do not think they will be caught.

While this may be true in some cases, we must remember that chilling effects can grip large numbers of individuals in their sphere of influence because of institutional application. We can readily hypothesize a realistic example in an educational setting. Suppose a high school teacher wishes to show a thirty-second clip of a two-hour access and copy-protected DVD as part of a class lecture. The present section 43(2) of the CO creates a fair dealing exception for showing a copyrighted film in the course of activities at an educational

---

37. Chloe Albanesius, *Study: 'Fair Use' Is Big Business*, PCMAG.com, Sept. 2007, http://www.pcmag.com/article2/0,1895,2183017,00.asp.

38. *Id.*

39. Defend Fair Use, http://www.defendfairuse.org/take_action.html (last visited July 31, 2007).

establishment.[40] Under a straightforward reading of this provision, this use of the DVD would not be infringing under current Hong Kong law. However, even with the chapter skipping function available on most DVDs, queuing up to the right part of the DVD can be tedious and time-consuming. So, suppose instead that in order to save time and make the class presentation more efficient, the teacher used a freely available DVD-rip program such as MacTheRipper[41] on her home computer to extract the same thirty-second section. The MacTheRipper software, like many similar programs, bypasses copy protection TCMs on DVDs.[42] Having extracted the clip, the teacher then embeds it into a PowerPoint presentation.

In this second version of the hypothetical, though the intent and effects are exactly the same, the teacher has violated the anticircumvention provisions in the amendments to the CO, opening herself, and quite possibly the school, to civil suit. This is also the result of a straightforward analysis of the relevant legal provisions. The difference is that clearly distinguishing the two situations and their legal ramifications requires a lengthy explication of the background legal principles—which is itself tedious, time-consuming, and above all expensive. A school could set a simple policy regarding DVDs to the effect that they can only be played if there is no "circumvention" of any sort—just buy a legitimate copy and play that one. But what about clips downloaded from the Internet? Or streaming media protected by a bundled-player program that has TCMs that are only applicable in certain situations? What about TCM-protected music clips that can only be played on the computer they were downloaded on? If the school were to develop a rule for each possible situation, the number of rules would rapidly become unwieldy. Given that lawsuits are also expensive, the rational choice for school administrators is to prohibit any use of a copyright work protected by TCMs, other than what is clearly allowed by an express licensing agreement with the copyright owner.

Given that copyright owners are typically in the business of licensing their works for a fee, at the end of the day the teacher will still teach, and the students will still get to see the clip, etc. One thing is missing from this picture, however: fair dealing. Because of the

---

40. Copyright Ordinance, (1997) Cap. 528, § 43(2) (H.K.).

41. Wikipedia.org, MacTheRipper, http://en.wikipedia.org/wiki /MacTheRipper (last visited Sept. 5, 2008).

42. *See* wikepedia.org, Macrovision, http://en.wikipedia.org/ wiki/Macrovision (last visited Sept. 5, 2008).

practical aspects of dealing with TCMs, fair dealing, and the public policy goals it supports, have been "circumvented."

Admittedly, this is not a situation of impending destruction. The harm from this change in the law manifests in reduced growth, transaction costs that burden free expression, and a transfer of wealth from the public to content owners via licensing fees. It will only be perceptible in the aggregate, and even then with some difficulty; a world of shriveled opportunities only truly visible in comparison to a hypothetical world where the public policy underlying fair dealing is allowed to operate unhindered.

III. CRYPTOGRAPHY AND SECURITY: INSUFFICIENT EXCEPTIONS

In this Part I will consider the potential effects of the anticircumvention amendments on cryptography and other forms of security research and innovation, again drawing on U.S. experience with the DMCA. These fields stand apart from the general domain of fair dealing because the amendments to the CO, like the DMCA, make specific exemptions for these activities. As we will see, however, there is ample reason to be concerned.

A. Locking Up Crypto

1. The Statutory Scenarios

First, let us consider in greater detail the amendments to the Hong Kong CO that restrict the use of a circumvention "device," defined therein as

> any device, product, component or means—
> (a) which is promoted, advertised or marketed for the purpose of the circumvention of the measure;
> (b) which has only a limited commercially significant purpose or use other than to circumvent the measure; or
> (c) which is primarily designed, produced or adapted for the purpose of enabling or facilitating the circumvention of the measure;[43]

Section 273B creates a concurrent civil remedy for copyright owners and their licensees against anyone who: sells, or for sale or hire makes, imports, rents, offers, exposes, or advertises such a device; exhibits, possesses, or distributes one in the course of any business; "distributes (otherwise than . . . in the course of any . . . business) any relevant device

43. Copyright (Amendment) Ordinance 2007, Ord. No. 15 of 2007, at A779, A783 (H.K.), *available at* http://www.legco.gov.hk/yr06-07/english/ord/ord015-07-e.pdf.

to such an extent as to affect prejudicially the owner of the copyright; or . . . provides any [circumvention] service."[44]

Section 273C, which varies somewhat from 273B, makes it a criminal offense to make a circumvention device for sale or hire; export one from Hong Kong for sale or hire; sell, rent, or try to sell one in the course of any business; exhibit one to the public in the course of a "circumvention business"; possess one with the intent that it be sold, hired, or exhibited in the course any business; or provide a circumvention service in the course of a circumvention business.[45] Conviction can result in fines up to $500,000 and four years imprisonment.[46]

With this in mind, let us turn to the cryptography exception, which is actually a combination of exquisitely complicated and convoluted exceptions to 273A, 273B, and 273C (the security testing exemptions will be considered in Part III.B, *infra*), which are scattered across 273D, 273E, and 273F.[47] When the different pieces of the exception are put together, what emerges is a set of three inoffensive scenarios envisioned by the drafters of the amendment. In the first scenario, a researcher at an official, Hong Kong Government-recognized educational institution circumvents a TCM for the sole purpose of cryptography research on behalf of the educational institution, or as part of taking or giving instruction in a cryptography course. This will not violate the anticircumvention provisions, provided that the research does not infringe copyright; the act is necessary in order to conduct the research; any information derived from the research is disseminated only in a way reasonably calculated to advance cryptography-related knowledge; and neither the act of circumvention nor the dissemination of research information prejudicially affects the copyright owner's interests.

In the second scenario, any regular person doing cryptography research who circumvents a TCM for the sole purpose of that research will not be liable, provided that the research does not infringe copyright; the act of circumvention is necessary for the research; and neither the act, nor the dissemination of research information prejudicially affects the copyright owner's interests.

In the third scenario, a third party is working collaboratively with someone who is conducting cryptography research. That third party will not be held liable for making, importing, exporting, selling, renting, distributing, or possessing a circumvention device, or providing a

44. *Id.* at A777-A779.
45. *Id.* at A781-A785.
46. *Id.* at A785.
47. *See generally id.* at A785-A801.

circumvention service to the researcher while collaborating with that researcher, as long as her purpose is to enable the researcher to commit an exempted act of circumvention envisioned in one of the first two scenarios. Basically, this is a "research assistant" exception.

2. What's Wrong with This Picture? Ask, But Don't Tell

A cursory glance at the scenarios envisioned by the drafters shows that they were thinking about cryptography research in both academic and nonacademic settings. Cryptography scientists and their research assistants can go about their educational activities, and the average crypto buff can tinker in her home workshop. However, careful attention to the interstices in the provisions reveals a gaping hole: the benefits of any research must remain locked away in ivory towers.

The drafters' statutory regime seems to give cryptography professionals and home crypto buffs express permission to publicly disseminate the results of their research.[48] Unfortunately, this permission is also expressly limited by the requirement that the disclosure not be prejudicial to the interests of the copyright holder.[49] This is a significant problem because as a practical matter, almost *any* dissemination of cryptography research results will be prejudicial to the copyright owner for the simple reason that it teaches people how to crack whatever TCM the crypto is embedded in. The only way public dissemination would not be prejudicial is if the crypto being researched is not actually being used in copyright TCMs (in which case the anticircumvention provisions would not even be applicable).

Thus, this inherent vagueness of "prejudice" in the cryptography research exception threatens to hamstring cryptography research in Hong Kong right out of the gate. Not all of it, though. There will remain a fair amount of cutting-edge cryptography research to be done on encryption methods not yet implemented in copyright-protecting TCMs. For example, in 2007, the U.S. government released a new official standard for random-number generators (RNGs).[50] RNGs are critical for implementing cryptography in real world applications.[51] One of the approved techniques in this standard has been questioned on the theory

48. *See id.* at A787-789.

49. *Id.* at A787.

50. Bruce Schneier, Did NSA Put a Secret Backdoor in New Encryption Standard?, WIRED, Nov. 2007, http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115.

51. *Id.*

that it might contain a U.S. National Security Agency "backdoor."[52] Crypto experts in Hong Kong would serve the public interest by putting their research efforts into exploring the reliability of the RNG techniques in the new standard. Hong Kong researchers could participate in this laudable research up until hardware and software developers around the world actually begin to follow the new standards, at which point anything Hong Kong researchers publish on the subject would run the risk of leading to civil liability.

This problem manifests itself in another manner. In the world of research, in an ivory tower or outside, one cannot simply make the unsubstantiated claim "I broke your crypto." It is standard practice to prove that the claim is true, often by supplying an explanation of the algorithm in the form of computer code that actually cracks the crypto.[53] Making the code available for public review, which in the modern world means putting it on the Internet, would be even more prejudicial than publishing a general description of it because the means/device that actually does the circumventing would be available worldwide to anyone, anywhere, who wanted to test the research.

Cryptography researchers have another reason to be concerned about these provisions. The making and publication of the code would be tantamount to making and distributing a "means" or "device" for circumventing a TCM. And, while 273E and 273F exempt the researchers and assistants who collaborate with a cryptography researcher from means/device liability,[54] if the amendments are read literally they do not exempt the researcher herself. In other words, if the amendments are followed to the letter, a researcher can think up a method of circumvention, and she can commit an act of circumvention for research purposes, but she cannot write her own code. That would violate the section 273B provision against "making" a circumvention device.[55] She must rely on her collaborating research assistant or another researcher exempted by 273E and 273F to write a piece of code to implement the idea so she can then commit the act exempted by 273D; in the alternative, she could write it herself and give it to another researcher with whom she is collaborating so that person can test it.[56] The

---

52. *Id.*

53. *See* Decl. of Bruce Schneier, Case No. CV-01-2669 (GEB), ¶ 14, Felten v. RIAA, (N.J. Dist. Ct., Aug. 14, 2001), *available at* http://w2.eff.org/IP/DMCA/Felten_v_RIAA/20010813_schneier_decl.html.

54. *See* Ord. No. 15 of 2007, *supra* note 8, at A795, A791-A801.

55. *See id.*

56. *See generally id.* at A787-A801.

anticircumvention amendments, it seems, will require that cryptography researchers work in pairs.

Unfortunately, none of these individuals will be able to publish the code and prove they are correct. Nowhere in the amendments are the collaborators or the original researcher exempted from liability for distributing an anticircumvention means or device for any reason (other than to each other). The dissemination exemption for the original researcher in 273A, strictly speaking, only covers the "information" that results from an act of circumvention,[57] and if the term "information" is not narrowly construed, the statute becomes internally self-contradictory. The making of a circumvention device by a collaborator exempted by 273E and 273F, i.e., writing the code, does not extend to dissemination to the public.[58] If the original researcher received this code from a collaborator and decided to publish it, she would still at least be disseminating an anticircumvention device within the meaning of 273B, and again, public dissemination of such a device is not exempted by 273E and 273F.[59] So, while she might be able to explain generally what tools she used in her cryptography research, once again she would not be able to do so at a level of detail that would permit someone to repeat the work.

3. Experience Teaches

One might object that even though the statutory cryptography exceptions contain some problematic wording, surely copyright owners would not wield civil suits against legitimate researchers. Unfortunately, judging from the U.S. experience with the DMCA, the reality is that they certainly will. Moreover, corporate copyright owners may have an obligation to stifle such research.

In September 2000, the Secure Digital Music Initiative (SDMI), a multi-industry group that develops TCMs for digital music, issued a public challenge inviting efforts to crack its "digital watermark" technology.[60] A team of researchers led by Princeton computer science professor Edward Felten took up the challenge and successfully defeated the TCM.[61] When the researchers tried to present a paper documenting their results at an academic conference, however, the researchers, their employers, and the conference organizers received letters from the

57. *See id.* at A787.
58. *See generally id.* at A787-A801.
59. *See id.* at A777-A781, A787-A801.
60. Electronic Frontier Foundation, *supra* note 26, at 2.
61. *Id.*

Recording Industry Association of America (RIAA) threatening legal action under the DMCA.[62]

Like the Hong Kong anticircumvention amendments, the DMCA does create an exception for cryptography research that includes the possibility of disseminating information gained from such research, subject to a restriction that such dissemination be made in a "manner reasonably calculated to advance the state of knowledge or development of encryption technology," rather than in a manner that "facilitates infringement."[63] Nevertheless, the RIAA position was that because the watermark was already implemented in actual products (a necessary prerequisite for the DMCA to be applicable), then good faith dissemination of the method used to crack that TCM at an academic conference could have "significantly broader consequences and could directly lead to the illegal distribution of copyrighted material."[64] In other words, *any* public dissemination would be prejudicial.

After lengthy discussions with counsel the researchers withdrew their paper from the conference.[65] In a public statement, Professor Felten explained why they backed down in the face of the DMCA threat: "Litigation is costly, time-consuming, and uncertain, regardless of the merits of the other side's case. Ultimately we, the authors, reached a collective decision not to expose ourselves, our employers, and the conference organizers to litigation at this time."[66] Portions of the team's research were eventually published at a later conference after the researchers filed a lawsuit and the DMCA threats were withdrawn.[67]

The worst-case scenario is quite severe. When the anticircumvention amendments come into effect, Hong Kong will become another jurisdiction where cryptography researchers will be subject to suit for doing cryptography research, and legitimate researchers will be hauled before the courts. Certainly, all will not be lost. Cryptography implementations have already gained great importance across Asia.[68] Public key technologies, for example, are employed in applications that range from the delivery of government

---

62. *Id.*

63. *See* 17 U.S.C. § 1201(g) (2000).

64. *See* RIAA Letter to Professor Edward Felten, http://cryptome.org/sdmi-attack.htm (last visited Nov. 27, 2007).

65. Electronic Frontier Foundation, *supra* note 26, at 2.

66. Statement of Professor Edward Felten, *available at* http://cryptome.org/sdmi-attack.htm (last visited Nov 27, 2007).

67. Electronic Frontier Foundation, *supra* note 26, at 2.

68. *See generally* Alana Maurushat, *Multi-Lateral Recognition of PKI Certification Authorities in the Asian Region: Transborder Data Flow and Information Privacy Issues*, 35 HONG KONG L.J. 569 (2005).

services to banking transactions.[69] So, there will always be some cryptography applications that are not being used in copyright TCMs; if there is any overlap, cryptography researchers can simply change fields. And, at the end of the day, crypto researchers and home crypto buffs can still do their research. They can—in pairs—explore, investigate, and expose dangerously weak implementations of cryptography used in critical government infrastructure and Britney Spears albums alike—just as long as they do not tell anyone about it.

Of course, the worst-case scenario is unlikely to come to pass: a reviewing court in Hong Kong would likely peer beyond the literal incongruities of the amendments and try to create a realistic amount of breathing room for legitimate research. However, even if we assume that the courts will be generally favorable to defendants in such cases, the potential for chilling effects is quite real, and the *Felten* case is an example that risks repetition. We must remember that many of the TCM-using copyright owners will be corporate entities. When a statute grants a corporation an advantageous entitlement, that corporation has an obligation to its shareholders to at least consider taking advantage of the entitlement. In the exercise of their business judgment, some corporate entities may decide that using the CO amendments to prevent disclosure of cryptography research results is not in their interests, and not avail themselves of the statutory protections. However, in the *Felten* case in the United States, a corporate entity came to the opposite conclusion.[70] Therefore, we must consider it a real possibility that, in the interests of protecting proprietary TCM technology and valuable copyrights, some corporations operating in Hong Kong will come to the same conclusion.

B. Security Testing: Similar Exception, Similar Problem, Unsurprising Results

1. The Statutory Scenarios

The second area of concern is computer security testing. In the world of TCMs that protect digital copyright, there is a significant amount of overlap with the issues raised in the cryptography section above. The difference here is that the situation is perhaps even worse. When it comes to security testing and Hong Kong's anticircumvention amendments—you are on your own.

Once again, a cursory look at the security testing exception as implemented in the amendments indicates that the drafters were

69. *Id.* at 570.

70 *See* RIAA letter to Professor Felton, *supra* note 65.

conscientiously attending to the vital need for unfettered computer security testing. As with the cryptography exception, careful excision and reassembly of provisions scattered across 273D, 273E, and 273F reveal the acceptable TCM circumvention situations envisioned by the drafters. Here there are essentially two. In the first, the owner or administrator of a computer or network, or her authorized agent, circumvents a technological measure for the sole purpose of testing, investigating, or correcting a security flaw.[71] In the second, an authorized person working collaboratively with the owner/administrator provides a circumvention service, or makes, imports, exports, sells, rents, distributes or possesses a TCM circumvention device for the purpose of enabling the owner/administrator to commit the security-testing circumvention.[72]

Based on the discussion above of the cryptography collaboration provisions, we can see the same problem in the scope of the provisions: the statute seems to require that people work in pairs if there is any sort of device or service involved. In other words, the literal wording of the statute does not permit the owner/administrator to make or acquire a circumvention device on his own—only collaboratively.

Again, there are additional grounds for concern.

2. Experience Teaches v2.0

a. A Threat to Science

The Hong Kong anticircumvention provisions pose a threat to scientific research.[73] It is quite clear from the two scenarios envisioned by the drafters that computer security research is entirely absent from the picture. The academic aspect present in the cryptography exception has disappeared from the drafters' imaginings—instead, they foresaw the need to circumvent copyright TCMs for purposes other than cryptography research as being limited to a trip to the tech support desk. Meanwhile, a huge amount of legitimate research in computer science departments around the world focuses on the myriad forms of computer security and everyday glitches that do not involve cryptography, so this is a significant omission. The untold numbers of computer hobbyists who, as a whole, discover and publicize a significant percentage of the most dangerous security glitches are likewise targeted.

---

71. *See* Ord. No. 15 of 2007, at A785-A887.

72. *See id.* at A791-A799.

73. *Cf.* Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, SCIENCE MAGAZINE, (Sept. 14, 2001) 10.1126/science.1063764, *available at* http://www.sciencemag.org/cgi/content/full/293/5537/2028?ijkey=sJ5V2ve/PTGkU (last visited Nov. 26, 2007).

A proponent of the amendments might still be tempted to rely on the reputation of scientific research and the good graces of the content owners. Perhaps the *Felten* controversy was a onetime problem, and surely SDMI, the RIAA, and similar industry groups learned their lesson from the ensuing backlash?

Not so. The DMCA contains a security testing exception that in substance is very similar to the exception contained in the Hong Kong amendments.[74] Thus, for a glimpse into the amendments' potential effects on legitimate research, we can again consider the U.S. experience, which has been dismal. The DMCA has repeatedly been used to block publication of legitimate security testing research, or otherwise harass legitimate researchers.[75] In one case in 2003, representatives from educational software company Blackboard Inc. cited the DMCA in a cease-and-desist letter used to stop students from presenting research on flaws in Blackboard's ID security system used in universities.[76] In another example from that same year, executives from SunComm threatened a DMCA lawsuit against a Princeton graduate student who published a report revealing that simply holding down the "shift" key on a Windows PC would render a SunComm CD TCM ineffective.[77]

The most notorious example of this use of the DMCA is probably the *Sklyarov* controversy. Dimitry Sklyarov, a Russian programmer, helped develop a program that allowed owners of Adobe eBooks to circumvent its TCMs and convert the eBooks into PDF files.[78] Among other things, the program was marketed for "making eBooks compatible with screen-reading software used by the blind."[79] When Sklyarov came to the United States in July 2001 to present a talk on the flaws in the eBook format, "he was arrested at the behest of Adobe Systems" and charged with a criminal violation of the DMCA.[80]

The consumer backlash was severe and Adobe quickly changed its stance and called for Sklyarov's release.[81] Nevertheless, Sklyarov spent three weeks in jail, and was only allowed to leave the United States several months later—after he agreed to testify against his employer,

---

74. *See* 17 U.S.C. § 1701(j), § 1201(j) (2000).
75. *See generally* Electronic Frontier Foundation, *supra* note 26, at 2.
76. *Id.* at 3.
77. *Id.*
78. *Id.* at 4.
79. Lee, *supra* note 26, at 19.
80. *Id.*
81. *Id.*

Elcomsoft, in a subsequent prosecution.[82] Elcomsoft was then acquitted by a jury.[83]

The fallout from the *Sklyarov* debacle combined with the fallout from the *Felten* controversy. Highly respected researchers such as Niels Ferguson stopped publishing research on copyright TCM security flaws on the grounds that they frequently traveled to the United States.[84] Others, such as network security protection expert Dug Song, removed information on computer security vulnerabilities from their websites out of fear of DMCA prosecution.[85] "Some foreign scientists have advocated boycotting conferences held in the United States, and some conference organizers have decided to hold events in non-U.S. locations. Russia went so far as to issue a travel advisory to Russian programmers traveling to the United States."[86]

b. A Threat to Consumers

Finally, but no less importantly, Hong Kong's anticircumvention amendments pose a threat to consumers. Under a strict reading of the amendments, cryptography researchers and even regular computer users who discover security flaws could publicly announce their existence, and simply withhold explanations of the code that substantiates and exposes the flaws. If the sources were sufficiently reputable, people might believe them on their word alone, without any explanation. Theoretically, members of the public could then contact the copyright owners who distribute the flawed TCMs and demand repairs of what they have been led to believe might be broken. Once enough consumers accepted the unsubstantiated claims and acted upon them, the copyright owners would act.

As a mechanism for dealing with computer security flaws, this is somewhat far-fetched.

Now, another possibility is the people who discover these flaws could notify the TCM developers about them. This is a form of relying on the good graces of technology companies that market TCMs, and players like SDMI and the RIAA (all of which are also the types of entities that have threatened to sue legitimate researchers). Unfortunately, U.S. experience shows that we cannot rely on the TCM developers to fix the problems of which they are aware.

---

82. *Id.*
83. *Id.*
84. *See* Electronic Frontier Foundation, *supra* note 26, at 4.
85. *Id.*
86. *Id.*

In 2003 and 2005, Sony-BMG released music CDs with two different TCMs that, unknown to users, also installed "cloaked" software on users' computers.[87] Once installed, the software quietly monitored customers' music listening habits and sent the information to Sony-BMG over the Internet.[88] Both TCMs created security vulnerabilities on the users' computers; the 2005 software included a "rootkit" that was particularly egregious.[89] Sony-BMG was notified of these vulnerabilities at least by September 30, 2005, but it did not publicize the information.[90] When the details of vulnerabilities were publicized by an independent researcher a month later, Sony-BMG did not immediately take any effective steps to provide removal tools.[91] Meanwhile, the millions of CDs containing dangerous Sony-BMG TCM software spread the infection to "at least 568,200 public, private, educational, and military networks worldwide,"[92] and the first known virus exploiting the vulnerabilities appeared on November 10, 2005.[93] Sony-BMG finally released information on methods for removing the dangerous TCM software on December 6, 2005—after "a number of individual and class action lawsuits were filed throughout the United States and other countries."[94]

Although the Sony-BMG "rootkit" scandal is the most notorious example of a TCM developer failing to publicize and correct a serious TCM security vulnerability in an expedient manner, it is not an isolated case.[95] From the TCM developer's perspective, these results are unsurprising: developers and distributors of TCMs have strong incentives not to publicize or correct problems. Public acknowledgment of security flaws is embarrassing, bad for company goodwill, and shakes consumer faith in TCMs. This in turn hurts sales and stock prices—and product recalls are extremely expensive. If a developer can get away with hiding the information for a few years, changes in computer technology could make the vulnerability obsolete—then only the

---

87. Mark H. Lyon, *Technical Protection Measures for Digital Audio and Video: Learning from the Failure of Audio Compact Disc Protection*, 23 SANTA CLARA COMPUTER & HIGH TECH. L.J. 643, 647-48 (2007).

88. *Id.* at 648-49.

89. *See id.*

90. *Id.* at 650.

91. *See id.* at 650-52.

92. *See id.* at 649-51.

93. Rebecca Jeschke, *New Virus Exploits Sony-BMG Rootkit*, ELECTRONIC FRONTIER FOUND. (Nov. 10, 2005), *available at* http://www.eff.org/deeplinks/2005/11/new-virus-exploits-sony-bmg-rootkit.

94. Lyon, *supra* note 87, at 652-53.

95. *See, e.g.*, Electronic Frontier Foundation, *supra* note 26, at 3.

developer and the hackers that take advantage of the security flaws would know of their existence. The developer may also calculate that the benefits it reaps from controlling users' music consumption with a TCM outweighs its potential civil liability—especially because it would be hard to prove that any given security breach was the fault of Sony-BMG. In the case of the Sony-BMG class action lawsuits, liability was predicated on potential danger[96]—not the extent of actual damage from the security vulnerabilities, which is unknown.

In the world envisioned by the anticircumvention amendments, corporate entities will probably survive TCM-related security flaws without too much difficulty. They will have access to in-house or third-party tech support, and can otherwise absorb damage with insurance. Researchers and independent security experts will be able to engage in security testing and detect flaws, but they will not be able to substantiate claims—their only audience will be the TCM developers. Most consumers, however, will have insufficient tech-support resources and computer savvy to participate in the security testing exception; they will be left to fend for themselves.

IV. CONCLUSION

The Hong Kong anticircumvention amendments contain significant problems that require attention. They threaten fair dealing rights in Hong Kong because they unduly expand the power of copyright owners to control the actual use of their works, rendering fair dealing rights moot. Although the amendments provide exceptions for cryptography and security testing, the wording of the exceptions is problematic, and U.S. experience with very similar provisions in the DMCA shows that they will nevertheless chill legitimate research and harm consumers.

The Administration was right in attempting to balance the multitude of copyright interests. However, judging from the U.S. experience with the DMCA, the amendments as written will not achieve this balance. Instead, the amendments overwhelmingly favor copyright owners, and place fair dealing rights, legitimate research, consumer digital security, and the public good at risk.

The purpose of Article is to draw attention to these issues and fuel continuing debate. Some of the problems identified in this Article could be resolved by careful judicial interpretation that attends to the underlying intent of the Administration. The more serious problems may

---

96. *See, e.g.*, Class Action Complaint, 05 CV 10190, (S.D.N.Y. 2005), *available at* http://www.eff.org/files/filenode/Sony-BMG/NY_complaint.pdf (last visited Nov. 27, 2007).

require additional amendments to prevent harmful outcomes, particularly in the realm of chilling effects on fair dealing and legitimate research. The U.S. experience demonstrates that these issues should be addressed proactively—before Hong Kong has to learn its anticircumvention lessons the hard way.