Final Draft

21st Century Copyright Reform: Adding Privacy Considerations Into the Normative Mix

Professor Emeritus Doris Estelle Long, The John Marshall Law School (Chicago)
Prof.doris.long@gmail.com

IN MAKING COPYRIGHT WORK FOR THE ASIAN PACIFIC?: JUXTAPOSING HARMONISATION WITH FLEXIBILITY (ANU Press 2017)(co-editors Susan Corbett and Jessica Lai)(forthcoming)

Abstract
From innovations that allow the creation of new works through artificial intelligence to the voracious demands of the "Internet of Things" for content, we are in the midst of foundational shifts in the norms and assumptions governing copyright that require reforms of outdated laws to deal with the realities of the global digital environment of the 21st Century. To assure that these reconfigured norms deal effectively with today's realities and tomorrow's future possibilities, reform efforts in the Asia Pacific region must leave the comfort of the past and consider new inputs into the reformation process. One of those new inputs should include the impact of the protection of personal and data privacy on copyright protection issues.

With the heightened surveillance possibilities of drone photography and the rapid unauthorized dissemination of personal sexting images that often qualify as copyright protectable works, privacy protection has become inextricably linked with copyright laws. Adding privacy concerns to copyright reformation considerations could impact critical issues, including enforcement, fair dealing, authorial rights and distributional controls. It might not simplify the process. But the normative framework that arises from these considerations could provide a copyright regime that is not only forward-looking, but avoids the problem of obsolescence that has dogged earlier reformation efforts. Yet simply adding privacy issues into the copyright reform "mix" and adopting some of the norms discussed in this Chapter is only the first step. To create copyright laws that will survive the next technological revolution, we must create a harmonized reformation, a code that will assure that these critical normative changes are incorporated across borders. Merely creating a patchwork of reformed laws in some countries based on new privacy-informed regimes disserves the borderless realities of the digital environment. If we truly want to create copyright laws for the 21st Century, we must be brave enough to take on the entire task. Anything less will simply leave the work for another generation.

B. The Author/Subject Dichotomy
C. Drones, Surveillance and Data Collections
D. Fair Use, Fair Dealing and the Public Interest in Privacy.
E. Resolving the TPM Debate: Considerations of Personal Data Privacy in Access Debates
F. Distributional Controls, Transformations and Injunctive Relief
Conclusion

Introduction

There is no question that copyright norms have undergone a foundational shift over the past twenty years. From the advent of the "Information Superhighway" in the 1990s to the "Internet of Things" today, digital communications media have revolutionized the creation, dissemination and infringement of copyrightable works. As the hard goods world of books, films, records, painting and sculpture has been transformed into a digital one, the scope of protection for authorial rights has come under increasing scrutiny.

The new technology of the Digital Age has led to the creation of potentially new copyrightable forms of works that do not automatically fit within existing paradigms based on a hard-goods world. These new forms are as diverse as online video games, smart phone apps, streaming video, and personal health monitors. The former lock on distribution of new works by large corporate content providers has disappeared as amateur authors increasingly create and distribute their own digital content. As cross border communications replace former geographically-restricted telecommunications media, territorially-based, collective rights licensing agreements are more out-of-step with present business models. Similarly, as streaming media, public performance, and broadcast rights replace old reproduction-based models of uploads and downloads of digital files, gaps and missteps in coverage have become increasingly apparent. Perhaps most notably, enforcement in the digital environment has become glaringly problematic.

All of these changes have led to copyright reform efforts in countries as diverse as Australia, China, New Zealand, Singapore, South Korea, the European Union, Hong Kong, Japan, Canada and the United States. These efforts have been triggered by the unique challenges the digital environment has posed to the hard-goods based regimes of the Berne Convention for the Protection of Literary and Artistic Works, and the Agreement on Trade-Related Aspects of Intellectual Property Rights. Neither treaty limited its application to the hard goods world in fact. But their application over time has only demonstrated the gaps and inadequacies they share in facing the copyright challenges of the 21st Century. These inadequacies have been exacerbated by the failure to deal with the myriad personal and data privacy issues that increasingly arise as a direct result of the new technologies used to create and distribute copyrighted works in the digital environment. This Chapter is not intended as detailed analysis of present reform efforts, but will use examples of potential reforms incorporating critical new privacy based considerations that could be followed to create a workable, harmonized "code" of future norms that would allow Asia Pacific countries to take full advantage of the opportunities presented by the global digital environment while retaining protections for personal privacy and human dignity.

The present movement for domestic reforms internationally has been matched by a rise in new copyright-related treaties, such as the Marrakesh Treaty to Facilitate Access to Published Works by Visually Impaired Persons and Persons with Print Disabilities (Marrakesh VIP Treaty).[1] Numerous draft treaties are currently in discussion before WIPO, including the Draft WIPO Archive Treaty,[2] the Draft Broadcast Treaty,[3] and a Draft Treaty for the Protection of Traditional Cultural Expressions,[4] that are considering fundamental normative changes in international copyright limitations and exceptions based on a perceived gap between present treaties and the new technologies, including, respectively, practices that threaten access to information and content rights in broadcast signals, and indigenous people's rights to control their own heritage.

The major copyright multinational treaties dealing with the "new" phenomenon of the internet, the WIPO Copyright Treaty (WCT) and its related-rights companion, the WIPO Performances and Phonograms Treaty (WPPT), were executed over 20 years ago. Although the Beijing Treaty on Audiovisual Performances (AVPT), dealing with related rights for audiovisual performers and producers, was executed more recently in 2012, it largely followed the foundational norms for performances set forth in the WPPT.[5] Major domestic reforms, such as the Digital Millennium Copyright Act (DMCA)[6] in the United States and the EU Directive on the harmonisation of certain aspects of copyright and related rights in the information society (EU InfoSoc Directive)[7] also date from approximately the same period as the WCT and the WPPT. They have not been significantly altered since their respective dates of enactment. Perhaps even more notable

---

[1] Marrakesh Treaty To Facilitate Access To Published Works For Persons Who Are Blind, Visually Impaired, Or Otherwise Print Disabled, available at http://www.wipo.int/treaties/en/ip/marrakesh/ ("Marrakesh VIP Treaty").

[2] See Working Document Containing Comments on and Textual Suggestions Towards an Appropriate International Legal Instrument (In Whatever Form) on Exceptions and Limitations for Libraries and Archives, SSCR/ 26/3 (April 15, 2013), available at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_26/sccr_26_3.pdf. See also Treaty proposal on Limitations and Exceptions for Libraries and Archives (December 6, 2013), available at http://www.wipo.int/edocs/mdocs/mdocs/en/wipo_reg_cr_sin_15/wipo_reg_cr_sin_15_t_17.pdf.

[3] Working Document For A Treaty On The Protection Of Broadcasting Organizations, SCCR/27/2 REV (March 25, 2014). See also Revised Consolidated Text On Definitions, Object Of Protection, Rights To Be Granted And Other Issues, SCCR.34/3 (March 13, 2017).

[4] Draft Articles for the Protection of Traditional Cultural Expressions, WIPO/GRTKF/IC/34/6 (March 14, 2017) available at http://www.wipo.int/meetings/en/fulltext_mdocs.jsp?q=the+protection+of+traditional+cultural+expressions%3A+Draft+Articles.

[5] These norms included reliance on the performers' making available right for exclusive control; compare WIPO Performances and Phonograms Treaty ("WPPT"), Arts. 8 & 10 with Beijing Treaty on Audio Visual Performances ("AVPT"), Arts. 8 & 10; on the three-step test for exceptions and limitations; compare WPPT, Art. 16 with AVPT, Art. 13; and on technological protection measures to combat piracy; compare WPPT, Art. 18 with AVPT, Art. 15. Efforts to deal with new "environmental" issues such as web-casting were basically tabled.

[6] Digital Millennium Copyright Act, 17 U.S.C. §§512, 1201, diverse, available at https://www.copyright.gov/legislation/pl105-304.pdf ("DMCA").

[7] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society ("InfoSoc Directive").

for purposes of our analysis of the relevance of privacy issues to copyright reform for the digital environment, none of these instruments, including the AVPT, addressed the issue of the inter-relationship between copyright and privacy on the internet. Neither have subsequent efforts such as the Asia Pacific Copyright Code.[8]

The necessary question arises as to why now? What is different about today's digital environment that has suddenly sparked this long overdue evaluation of copyright boundaries? Part of the explanation is necessarily based on the need for sufficient experience with the reality of the altered circumstances of copyright utilization in the digital environment. Copyright reform always evolves more slowly than the technological changes in communications media it must address. For example, in the United States, the first photographs (daguerreotypes) were created in the late 1830s. Yet copyright law was not altered to acknowledge that works created using this new medium qualified for protection as original works until the Supreme Court decision, *Burrow-Giles Lithographic Co. v. Sarony*,[9] in 1884.

But I believe the most significant reason for the explosion in reform efforts currently is because technology has not resolved the challenges faced by copyright owners in the digital environment. Early hopes that anticircumvention regimes would provide adequate protection for technological solutions to the unauthorized use of copyrighted works have proven evanescent, as pirate websites have grown exponentially.[10] The increased success of third parties in hacking technological protection measures, the rise of virtual private networks and dark nets that utilize encryption to protect *infringing* activity, and the proliferation of pirated works due to even newer reproductive technologies, such as 3-D printers, have created a renewed urgency for reform.

Yet as we deal with the new realities of copyright in the global digital environment, it is critical that we avoid the mistakes of the past. We must acknowledge that there are new inputs that must be considered as we create the normative foundations for copyright protection in the 21st Century.[11] One of those critical new inputs concerns both personal and data privacy. Such concerns are no longer adjuncts to issues of copyright protection but instead argue for new normative values as we reconfigure the boundaries of authorial control in this new era of access and transformation.

1. What privacy?

Privacy has no single definition internationally. The concept of privacy can include everything from the right to be left alone or "forgotten;" to the right to associational privacy; the right to avoid unwanted surveillance of either physical space or data; the right to a private space in one's own physical surroundings or in one's own mind (access

---

[8] Adrian Sterling, Draft Asia Pacific Copyright Code (2015), available at http://www.apcacopyright.org/conference-2015/conferences/copy-right-law-and-policy-in-the-asia-pacific-conference-2015.

[9] 111 U.S. 53 (1884).

[10] Insert cite to Susan's chapter.

[11] Insert cite to Lida's chapter.

to information); the right to control the dissemination of one's unpublished works or images of private lawful activities; or the right to control the disclosure and use of personal identifying information and personal information.[12]

This last category of "privacy" has received the most attention in recent years. As used here, the term "personal identifying information" is meant to include any information that can be used to identify an individual, directly or indirectly. Such information includes traditional categories, such as a name, address and social security number, as well as newer methods of source identification such as DNA and other biometric information, digital footprints, aggregated data, and other aspects of so-called "Big Data" that can be used to determine identity. This broad definition of privacy is intended to be co-extensive with, but not necessarily limited by, the definition for "personal data" contained in the European Union General Data Protection Regulation. (GDPR)[13] in South Korea's Personal Information Protection Act (PIPA),[14] and for "personal information" contained in China's 2016 Cybersecurity Law.[15]

Under the GDPR, protected "personal data" includes "any information relating to an identified or identifiable natural person (data subject)."[16] An "identifiable natural person" is "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[17] South Korea's PIPA defines "personal data" even more broadly to also include "information pertaining to any living person that makes it possible to identify such individual by his/her name and resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information)."[18] China's definition of "personal information" under its new Cybersecurity Law reflects a similarly open-ended approach by including "all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses, telephone numbers, and so forth."[19]

---

[12] See generally Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890). See also Doris Estelle Long, Is a Global Solution Possible to the Technology/Privacy Conundrum,? in Through the Technology Lens, 4 J. Marshall Rev. Intell. Prop. L. 6 (2005).
[13] European Union, General Data Protection Regulation, (2016/679), Art. 4(1)("GDPR").
[14] Republic of Korea ("South Korea"), Personal Information Protection Act, Art. (2011)("PIPA").
[15] People's Republic of China ("PRC"), 2016 Cybersecurity Law, Art. 76(5). Under Article 79, the effective date of China's Cybersecurity law was June 1, 2017. Due to strong criticism, the enactment of the provisions regarding cross-border transfer and data retention have been delayed. The effective date for the remaining provisions, including the NTD provisions, however, remains unchanged at the time this Chapter was completed. China Postpones Portion of Cybersecurity Law, The New York Times (May 31, 2017), available at https://www.nytimes.com/aponline/2017/05/31/world/asia/ap-as-china-cybersecurity-law.html?_r=0.
[16] Id.
[17] Id.
[18] PIPA, Art. 2(1).
[19] PRC, 2016 Cybersecurity Law, Art. 76(5).

Yet in the interstices between copyright and privacy and, in particular, in the normative spaces addressed in this Chapter, "privacy" is not simply limited to identifying data, no matter how broadly defined. To the contrary, other aspects of "privacy" that relate to a sense of personal control over one's space and actions (surveillance) or to one's image or works (unauthorized publication or dissemination) are equally relevant in creating viable copyright norms for the 21st Century. Such spatial or informational privacy includes considerations regarding the unauthorized dissemination of private correspondence or images of private sexual activity. In the context of the internet, it also includes the right to avoid the collection of personal information about one's web viewing or reading habits.[20]

In addition, corollaries to securing spatial and informational privacy are also relevant in the creation of copyright norms. These corollaries include the protection of encryption and other technological methodologies to secure privacy rights in the Digital Age and their unauthorized breach through such efforts as hacking, phishing and cyber espionage. They also include content-based privacy concerns from other legal regimes such as protection against "sexting" and "revenge porn."

The purpose of this wide-ranging definition is not to provide an all-inclusive list of topics to be covered within the context of copyright reform. Instead, it is to underscore the need for an approach that welcomes and actively seeks other normative inputs in creating the next generation of global copyright regimes. It is only through a fluid and more flexible approach that we can assure a more appropriate and sustainable future copyright regime for the Digital Age, and beyond.

2. Breaching the Copyright/Privacy Wall

Even in the pre-digital era, the wall between copyright and privacy regimes was not an absolute one. To the contrary, data privacy concerns often arose in the context of securing information regarding the identity of the manufacturers and distributors of pirated goods. Courts routinely balanced the need for such disclosure as a matter of legal relevance with an individual's right of privacy. The need for identity disclosure became even more severe with the explosion of pirated works distributed through early peer-to-peer networks such as Napster and Kazaa. It has continued apace as anonymizer technologies have made the securing of such information even more difficult. As requests for end user identities increased, privacy considerations were initially given relatively short shrift.[21]

---

[20] Unlike other countries, such as Australia, China, Japan, the Philippines, Singapore and the European Union which provide relatively strong protection regarding data collection practices; in the United States, such considerations may be more difficult to bring into present copyright reform discussions given recent Congressional action overturning such protections imposed by regulations passed by the Federal Communications Commission. Senate Joint Resolution 34, Public Law 115-22 (April 2017), available at https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34/text. Although there are other laws and regulations that provide partial protection for these activities, this recent legislative action undoubtedly makes the inclusion of such considerations as part the U.S. copyright reform highly problematic.

[21] See 17 U.S.C.§ 512(h)(establishing an identity disclosure subpoena process that mandated disclosure on good faith request).

For example, under the DMCA, the United States originally mandated end-user identity disclosures by affected online service providers (OSPs) without judicial oversight.[22] Over time, however, even in the United States, with its relatively limited protections for end user privacy generally, privacy protections have played an increasingly significant role in controlling such disclosures.[23]

The interconnections between copyright and personal privacy regimes are no longer limited to issues of identity disclosure. To the contrary, data privacy issues now affect such critical questions as the admissibility of evidence of infringing activity secured through the use of website scraper technologies and automatic takedown bots. In *Arista Records LLC v. DOE 3*,[24] for example, the court expressly held that the right to anonymity in internet communications could outweigh copyright interests in identity disclosure (although in this particular instance, privacy interests did not outweigh those of the copyright owner).

Similarly, the enforceability of injunctions blocking end user access to identified pirate websites is frequently decided by balancing personal privacy interests against copyright protections.[25] In brief terms, website blocking is achieved by a technological impediment, imposed by an OSP, that prevents end users from accessing designated pirate websites. Such blocks include "IP blocks" that prohibit access to specific internet protocol addresses, "DNS blocks" that block access to specified domain names, and proxy blocks that route the traffic on a site through a proxy server for filtering. The European Union, for example, has insisted on "proportionality" in balancing copyright and privacy interests when seeking to impose website blocking solutions to digital piracy.[26] Such proportionality does not prevent the enforcement of website blocking injunctions,[27] but it does make such relief more difficult to secure.[28] By contrast, in Australia, privacy issues are not expressly considered in determining whether a block should issue.[29] This approach may change, however, as Australia's efforts to establish broader rights to protect personal privacy continue.[30]

---

[22] 17 U.S.C.§ 512(h). See Discussion infra Part 3A.

[23] See London-Sire Records, Inc. v. Doe 1 Et Al, 542 F. Supp. 2d 153 (D. Mass. 2008); BMG Canada, Inc. v John Doe, 2004 Fed. Ct. Trial Lexis (Federal Ct. Canada 2004); Bonnier Audio AB v. Perfect Communication Sweden AB (Case C-461/10) (2012).

[24] 604 F.2d 110 (2d Cir. 2010).

[25] See Scarlet Extended v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (Case C-70/10) (2011).

[26] Id.

[27] See EMI Records Ltd & Ors v British Sky Broadcasting Ltd & Ors [2013] EWHC 379 (Ch) (28 February 2013).

[28] See Scarlet Extended v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (Case C-70/10)(2011).

[29] See Roadshow Films Pty Ltd v. Telstra Corporation Ltd [2016] FCA 1503 (15 December 2016).

[30] See Narelle Smythe & Morgan Clarke, A statutory cause of action for serious invasions of privacy on the way for New South Wales? (March 17, 2016), available at https://www.claytonutz.com/knowledge/2016/march/a-statutory-cause-of-action-for-serious-invasions-of-privacy-on-the-way-for-new-south-wales. See also Commonwealth of Australia, Issues Paper : A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy (September 2011).

Finally, even decisions allowing filtering to remove infringing content are impacted by privacy considerations.[31] Recent attempts to impose filtering obligations on OSPs through government or private regulation have been challenged because their application directly impacts end user privacy rights.[32]

Even activities perceived to be related to the traditional domain of privacy law, such as hacking, and surveillance, have increasingly intruded into the arena of copyright.[33] From the heightened surveillance possibilities of drone photography to the rapid unauthorized dissemination of personal information through the digital posting of leaked documents and personal sexting images, privacy has become inextricably linked with copyright. The first attempts to remove leaked information regarding membership in a website that promoted marital infidelity in the United States, Ashley Madison.com, was based on its purported violation of the copyright in the membership list.[34] Early efforts to remove photos of private consensual sexual activity, distributed without the participant's consent in cases of "sexting" or "revenge porn" in the United States have similarly focused on copyright and the ability to take-down infringing works.[35] In fact, such efforts have proven so popular that companies such as DMCA Defender have been created to help victims remove such items from the diverse array of internet sites, including Twitter, on which they can appear. New Zealand even has a specific provision in its 1994 Copyright Act under its moral rights chapter giving the subject of photos commissioned for private or domestic purposes the right to prevent their unauthorized public distribution, exhibition or communication.[36]

3. How Privacy Considerations Can Impact Copyright Reform

A. Reforming NTDs and Other Digital Enforcement Mechanisms

One of the most contentious issues facing copyright owners and the public today is the method used to remove infringing content from digital networks.[37] Regardless of

---

[31] See Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog (Case C-360/10)(2012).

[32] Jeremy Malcolm, Upload Filtering Mandate Would Shred European Copyright Safe Harbor (October 2016), available at https://www.eff.org/deeplinks/2016/10/upload-filtering-mandate-would-shred-european-copyright-safe-harbor (contending such regulations violate personal privacy and access to information provisions of the European Charter of Fundamental Rights).

[33] See Susy Frankel, The Copyright and Privacy Nexus, 36(3) Victoria U. Wellington Law .Rev. 507 (2005)(analyzing connections between privacy and, inter alia, unauthorized distribution of personal photographs).

[34] Hope King, Ashley Madison tries to stop the spread of its leaked data (August 21, 2015), available at http://money.cnn.com/2015/08/21/technology/ashley-madison-dmca-requests.

[35] See 17 U.S.C. § 512 (c). See also Ian Sherr, Forget being a victim. What to do when revenge porn strikes (May 13, 2015), available at https://www.cnet.com/news/forget-being-a-victim-what-to-do-when-revenge-porn-strikes.

[36] New Zealand, Copyright Act of 1994 §105 (as amended by the New Technologies Amendment of 2008 (Section 62(1)).

[37] In fact the NTD provisions of the US DMCA have already been the subject of four days of public roundtables and an on-going study by the U.S. Copyright Office, including two requests for public comments that have generated over 92,000 submissions to date.

the precise economic impact of digital piracy, there is no question that the proliferation of illegal content on the internet and on other digital platforms is the greatest challenge facing content owners. Most countries that have considered some form of a notice and takedown regime (NTDs) to alleviate the problem have achieved less than stellar results. Privacy considerations would not only place such takedown techniques in a different light, they would also provide unique insights into how NTDs can be reformed to achieve the balanced approach to protection between authors' and end users' rights they were originally designed to achieve.

Internationally, NTD procedures have evolved from the original Notice and Takedown procedures of the US DMCA,[38] to the "three-strikes" rule of the French Haute Authorité pour la diffusion des oeuvres et le protection des droits sur internet (Hadopi)[39], to the Notice and Notice provisions of the Canadian Copyright Modernization Act (CMA)[40] and variations of this new iteration of the "graduated response" to online piracy, including the "six strikes plus" rules of current private initiatives.[41] None has proven wholly satisfactory.

Under the DMCA, on receipt of an appropriate notice of infringement from a copyright holder, the OSP must take down the identified material or lose its safe harbor. Such takedown can occur either by actual removal of the identified material from the website or by disabling access to it. To secure content takedowns, copyright owners must provide a written notice containing identification information regarding the infringing material, including name and locational data,[42] along with a statement of good faith on the part of the copyright holder.[43] Where an OSP acts in good faith in response to a notice of infringement, it will not be liable so long as it promptly notifies the subscriber of its actions, provides the complaining party with any counter notifications it receives from the end user and replaces any removed material subject to a proper counter complaint within 10 to 14 days of receipt of the counter notice, *unless* the OSP receives notice from the original complaining party that it has filed a lawsuit regarding the material in

---

[38] 17 U.S.C. §512(c). Other countries that have adopted a similar notice and takedown process include, South Korea, South Korea, Copyright Act, Art. 103; Singapore, Singapore, Copyright Act, 193D; and the European Union, European Union, Directive on E-Commerce, 2000/31/EC (2000), Art. 14. The efficacy of this process, particularly where it lacks a stay-down requirement, has been severely criticized. See Devlin Hartline, Endless Whack-A-Mole: Why Notice-and-Staydown Just Makes Sense (January 14, 2016), available at https://cpip.gmu.edu/2016/01/14/endless-whack-a-mole-why-notice-and-staydown-just-makes-sense/. But see Elliot Harmon, "Notice-and-Stay-Down" Is Really "Filter-Everything (January 21, 2016), available at https://www.eff.org/deeplinks/2016/01/notice-and-stay-down-really-filter-everything.

[39] French Intellectual Property Code, Arts. L-331-25, et seq. (2009). Other countries that have adopted a similar "three strikes" graduated response include New Zealand and South Korea. New Zealand Copyright Act §§122B; South Korea, Copyright Act, Art. 133bis.

[40] Canada, Copyright Act, Art. 41.25 et seq. Other countries which have adopted a graduated response requiring notice and notice with no obligation of takedown absent a court order, and no limit on the number of notices (unlike the "three-strikes" rule), include Great Britain, United Kingdom, Digital Economy Act of 2010, Art. 124A.

[41] See Discussion infra Part 3A.

[42] 17 U.S.C. §512(c)(3).

[43] Id. They must also include an affirmation of accuracy. Id.

question.[44] Similar NTD provisions have been adopted by a variety of countries, including China, New Zealand, Singapore, and South Korea, however, the precise timing of such takedowns has varied.[45]

The efficacy of these takedown procedures has been hotly contested. Content owners criticize this process because there is no general obligation for OSPs to monitor content to assure that removed material is not re-posted. OSPs criticize the process because compliance has become extremely costly. According to Google's Transparency Report, it responds to over 2 million takedown requests a day.[46] End users criticize the process because it is frequently abused by copyright owners who seek to remove lawful material. Such removal is increasingly secured through the use of automated bots, which do not examine the material to determine if the use at issue qualifies as a fair or permitted one despite the legal obligation to do so in some countries.[47] Although, similar to other countries,[48] the NTD process under the DMCA allows end users to challenge unauthorized takedowns, present, incomplete studies and anecdotal evidence seems to indicate that only a small percentage of end users actually utilize the process.[49]

While the first generation of NTD regimes allowed for relatively rapid removal of infringing material, they did not end the cycle of notice, removal, re-post that these regime created (often referred to as a game of "whack a mole").[50] The "three strikes" rule of the French Hadopi, enacted in 2009, arguably resolved this problem by providing that end users who engaged in three instances of online copyright infringement within a specified period of time could have their *internet* access suspended for a period of up to one year.[51] Infringing acts were broadly defined to include the unauthorized reproduction, representation, distribution or communication to the public.[52] As opposed to a single notice, three notices were required before the potential suspension penalty could attach.[53] Ultimately, the threat of so draconian a penalty, along with the practical realities in

---

[44] Id. at §512(g).

[45] PRC, Network Regulations, Art. 15 (takedown must occur "promptly"); New Zealand, Copyright Act §92C (takedown "as soon as possible"), Singapore, Copyright Act, Art. 193D(2)(b)(iii)(OSP "expeditiously takes reasonable steps to remove or disable access."); South Korea, Copyright Act, Art. 103(2)(OSP must "immediately suspend the reproduction and interactive transmission; but see South Korea, Copyright Act, Art. 133bis (establishing a three strikes graduated response in certain cases). But see New Zealand, Copyright Act §122B (establishing three strikes graduated response for the issuance of enforcement notices intended to result in OSP account suspensions for alleged infringing file sharing).

[46] See Google Transparency Report, available at https://www.google.com/transparencyreport/removals/copyright/?hl=en#glance.

[47] See Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150 (N.D. Cal. 2008). For a further discussion of the relationship between fair use and NTDS, se Discussion infra Part 3A.

[48] PRC, Network Regulations, Arts. 16 &17; Singapore, Copyright Act, Art. 193DA.

[49] Daphne Keller & Annemarie Bridy, DMCA Counter-Notice: Does It Work To Correct Erroneous Takedowns (January 17, 2017), available at http://cyberlaw.stanford.edu/blog/2017/01/dmca-counter-notice-does-it-work-correct-erroneous-takedowns.

[50] "Whack-a-mole," refers to the general ineffectiveness of the present process. You may try to hit a mole, but it moves so quickly and disappears down holes so rapidly you cannot really hit one.

[51] French Intellectual Property Code, Arts. L-331-25 et seq (2009).

[52] Id. at, Art. L-336-3.

[53] Id. at Art. 331-26.

effectuating an actual suspension of access to the *internet* (as opposed to a single OSP) doomed the three strikes approach of Hadopi. In contrast to Hadopi's *internet* suspension approach, however, New Zealand's, South Korea's and Taiwan's three strikes approach were directed to suspension from a particular OSP's account.[54] In addition, New Zealand's law was directed expressly to instances of infringement based on "communication to the public."[55] By narrowing the scope of the access denial penalties, these laws arguably provided a more workable version of the three strikes regime.

In the next iteration of the graduated response NTD, Canada enacted Section 41.25 of the CMA,[56] establishing a "Notice and Notice" approach that further extended the time for removal of infringing material. The CMA does not require OSPs to remove identified infringing material. Instead, it obligates them to forward notices of infringement from copyright owners and retain end user identity information to turn over on court order to the copyright owner for subsequent legal action.[57] While this process improves end user education and eliminates the problem of abusive removals, its graduated response does not contain any rapid removal obligations, even at the end of the Notice cycle, without court action. The Notice and Notice approach has proven extremely popular. Subsequent private arrangements between content providers and OSPs, such as the "six strikes" agreement (Copyright Alert System), established in 2011 between various OSPs and content owners in the United States, including Verizon, AT&T, the Motion Picture Association of America and the Recording Industry Association of America,[58] and the Creative Content program in the United Kingdom[59] have followed a

---

[54] New Zealand, Copyright Act §122P; South Korea, Copyright Act, Art. 133bis; Taiwan, Copyright Act, Art. 90quinquies. To date, the suspension provisions of the New Zealand Copyright Act under Section 122P have not yet been brought into force. Section 122R requires enactment "by Order of the Council" which has not yet occurred. New Zeland Copyright Act, §122R.

[55] New Zealand, Copyright Act §122P. Unfortunately Section 122P has yet to be brought into force. See note 54 supra.

[56] Canada, Copyright Act, Art. 41.25.

[57] Id. at § 41.26. Similar identity disclosure obligations on court order exist under New Zealand's copyright law. See New Zealand, Copyright Act §§122J & 122Q (identity disclosure on Tribunal and Court order, respectively). The identity disclosure provisions by court order under Section 122Q are not yet in force. Id. at § 122R (requiring enactment by "Order of the Council" for this provision that has not yet occurred).

[58] See Copyright Alert System, Center for Copyright Information (2013), available at http://www.copyrightinformation.org/the-copyright-alert-system. In 2017 the Copyright Alert System was "concluded" with the statement that it "succeeded in educating many people about the availability of legal content, as well as about issues associated with online infringement." Id. Others suggested its "conclusion" was not the result of educational success, but of its failure to deal effectively with persistent infringers. See Jacob Kastrenakes, 'Six strikes' anti-piracy initiative ends after failing to scare off 'hardcore' pirates, The Verge (January 30, 2017), available at https://www.theverge.com/2017/1/30/14445596/six-strikes-piracy-system-failed-ending.

[59] See Creative Content, Home, available at https://torrentfreak.com/uk-piracy-alerts-the-first-look-inside-the-warning-system-170210. This program is currently known as "Get It Right from a Genuine Site." See Get It Right From a Genuine Site, Home available at https://www.getitrightfromagenuinesite.org. Notices under the "Get It Right" program reportedly were first issued in February 2017. See UK Piracy Alerts: The First Look Inside the Warning System, Torrent Freak (February 10, 2017), available at https://torrentfreak.com/uk-piracy-alerts-the-first-look-inside-the-warning-system-170210.

similar approach. In fact, the phrase "six strikes" appears a misnomer since there is no required takedown or account suspension after receipt of six notices of infringing conduct. As with the Notice and Notice approach of the CMA, content owners would have to seek takedown relief through the courts.

The trend toward delayed removal of infringing material from the internet in the most recent iterations of NTDs is problematic, given the rapidity with which material spreads in the digital environment. One of the reasons for the continued popularity of the NTD process under the DMCA in the United State has been its utility in dealing with non-copyright issues, such as removing fake mirror websites that mislead consumers, including shadow bank and consumer products sites. These shadow websites are often used to support phishing attacks, by securing personal information from unsuspecting consumers that can then be used in various criminal and fraudulent activities, including identity theft. NTD processes allow for a quick removal of such websites while investigations and court actions based on the fraudulent activity proceeds along a separate track. As noted above, DMCA NTD processes have also proven popular in removing sites that disseminate materials that violate individual privacy, such as the membership list from the Ashley Madison website.[60] Although other claims based on the illegal conduct that secured these lists, including violation of anti-hacking provisions under the Computer Fraud and Abuse Act,[61] might be used to secure similar relief, it would not be so quickly achieved.

While the need for swift removal of content based on its copyrighted nature might be subject to dispute, when privacy considerations are added into the normative mix swift removal becomes a viable and arguably even a necessary solution. But privacy issues also require a more nuanced approach to takedown since abuse could have serious effects beyond chilling free speech. Moreover, coverage decisions would not be made solely on the existence of copyright.

Where the subject matter or the circumstances surrounding dissemination raise privacy issues in connection with copyrighted materials, rapid takedowns serve a critical role in protecting personal rights. Pirated works generally cause monetary harm. By contrast, private diaries, surveillance videos, child pornography, cyberbullying, sexting and other content whose unauthorized dissemination violates personal privacy cause *emotional* harm. In some cases, such as revenge porn and cyberbullying, emotional harm is so severe that some subjects have committed suicide as a result of such unauthorized communications. The longer such content remains available on the internet, the greater the emotional harm. Rapid takedown may not fully eliminate emotional harm, but it certainly helps stop its growth.

Even under the takedown procedures that obligate removal of infringing material, rapid takedowns are not so rapid. Removal under Singapore's Copyright Regulations must occur within 14 days.[62] Other countries, such as China, Australia and the United

---

[60] See Discussion supra Part 3A.
[61] 18 U.S.C. §30.
[62] Singapore, Copyright (Flagrantly Infringing Online Location) Regulations 2014 §3;

States require "prompt" or "expeditious" removal.[63] New Zealand requires removal "as soon as possible."[64] None of these set forth a specific time frame for action.

In contrast, the New Zealand Harmful Digital Communications Act 2015 (HDCA) requires takedown by the OSP *within 48 hours* of receipt of appropriate notice from the affected subject.[65] The HDCA applies to "digital communications" that "cause serious emotional distress."[66] It is not a copyright statute, but it serves as a useful model for the types of privacy concerns that would be implicated if privacy considerations were included in the reformation of present NTD processes for copyrighted works. Among the harmful communications covered by the HDCA are cyberbullying, sexting and the unauthorized dissemination of "intimate visual recordings" made "without the knowledge or consent of the individual who is the subject."[67] To qualify as an "intimate visual recording" under the HDCA the image must have been made in "a place which, in the circumstances, would reasonably be expected to provide privacy."[68] A covered "digital recording" includes depictions and accompanying text concerning private sexual activity.[69]

The HDCA, similar to the DMCA, requires OSPs to forward copies of complaints to the end user and allows for counter notification to prevent removal or secure re-posting of the affected work.[70] Either party can also seek quick relief from Netsafe, the designated agency for reviewing complaints, and from the courts (after the required agency review).[71] This allows for a necessary safety net in cases of abusive or improper requests or OSP reluctance to remove end user content.

Privacy considerations would undoubtedly support the institution of some form of rapid takedown in copyright reforms at least for certain works. Given the content specific nature of the covered works -- they must violate the requisite privacy interests -- *actual* review prior to a subject's issuing a take down request would likely be mandated. Yet in some NTD processes, such content review is already required. For example, although the DMCA only requires that copyright owners make a "good faith declaration that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law,"[72] recent decisions have indicated that such "good faith" basis does not eliminate the obligation to review identified content for fair use exceptions. In *Lenz v. Universal Music Corp*,[73] the OSP had taken down a 29 second video containing of the

---

[63] PRC, Network Regulations Art. 15 ("promptly"): Australia, Copyright Regulations 1969, Regulation 20J ("expeditiously"); 17 U.S.C. §512(c)(1)(C)("expeditiously").
[64] New Zealand, Copyright Act § 92C.
[65] New Zealand, Harmful Digital Communications Act 2015, § 24 ("HDCA"). See Discussion infra Part 3B for an examination of the shift from author to subject ability to take down violative materials,
[66] Id. at § 24(2).
[67] Id. at § 4.
[68] Id.
[69] Id.
[70] Id.
[71] Id. at § 8.
[72] 17 U.S.C. § 512(c)(3).
[73] 801 F.3d 1126 (9th Cir. 2015).

defendant's young children dancing in the family's kitchen while a poor quality sound track of "Let's Go Crazy" by the artist known as "Prince" played in the background. The trial court found that Universal was obligated to consider whether Lenz's use of the song qualified as a fair one *before* seeking its takedown:

> Undoubtedly, some evaluations of fair use will be more complicated than others. But in the majority of cases, a consideration of fair use prior to issuing a takedown notice will not be so complicated as to jeopardize a copyright owner's ability to respond rapidly to potential infringements. The DMCA already requires copyright owners to make an initial review of the potentially infringing material prior to sending a takedown notice; indeed, it would be impossible to meet any of the requirements of Section 512(c) without doing so. A consideration of the applicability of the fair use doctrine simply is part of that initial review….[A] full *investigation* to verify the accuracy of a claim of infringement is not required.[74]

By using a good faith standard, the DMCA allows content owners to make good faith judgments about fair use without penalty. Leniency in harmful communications reviews would similarly give breathing space to subjects who seek good faith removal of such communications.

One of the difficulties with NTDs has been the potential for abuse. In response to a recent roundtable on reform held by the U.S. Copyright Office, Google identified several recent instances of abuse, including flooding an OSP with demands for removal for nonexistent websites to assure that all copies of an identified infringing work are removed from all potential locations, and a demand by a lawyer seeking removal of a blog post criticizing the lawyer for plagiarizing content on his website.[75] There are also countless examples of clearly acceptable instances of fair use/fair dealing that have been removed inappropriately.[76] The potential for abusive complaints could be even greater where the basis for takedown is its "harmful" nature. Allegations that an internet provider hosts such content could create significant reputational harm that is not generally present even in cases of pirate websites. To reduce such abuses, NTD reform would require strong penalties for knowingly making wrongful requests for takedowns.

Section 512(f) of the DMCA, for example, imposes damages, including costs and attorneys' fees against "any person who *knowingly materially misrepresents* … that material or activity is infringing."[77] The damages include those "incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a

---

[74] Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150, 1155-1156 (N.D. Cal. 2008)(emphasis in original), aff'd 801 F.3d 1126 (9th Cir. 2015).
[75] Google Reply to Section 512 Study: Request for Additional Comments, Docket No. 2015-7 (November 08, 2016), available at https: //regmedia.co.uk/2017/02/23/google-section-512.pdf.
[76] See Online Policy Group v Diebold Inc., 337 F.Supp.2d 1195 (ND Cal. 2004): Lenz v. Universal Music Corp., 801 F.3d 1126 (9th Cir. 2015). See generally Jennifer Urban et al, Notice and Takedown In Everyday Practice (March 2017), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628 ("Takedown Report").
[77] 17 U.S.C. §512(f)(emphasis added).

service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it."[78] Although Section 512(f) has been underutilized,[79] it represents an example of the type of penalty assurance required to reduce abuse of takedown rights.

While adding privacy concerns into copyright reform should give rise to a reconsideration of the importance of rapid takedowns, combined with penalties against abuse of such processes, the normative values derived from this exercise are not so narrowly circumscribed. To the contrary, by establishing a process that recognizes a content-based approach to rapid takedown, the use of this differential approach does not have to be so narrowly circumscribed. To the contrary, rapid takedown could also be established for works for which the economic harm of its unauthorized communication to the public is significantly greater than for other works. The clearest example would be commercial works that are in their pre-release periods, when the unique harm caused by their unauthorized release causes a special type of artistic harm. As Congressman Howard Berman of the U.S. House of Representatives recognized in supporting the Family Entertainment and Copyright Act of 2005, that established specific criminal penalties for the unauthorized distribution of copyrighted works "being prepared for commercial distribution"[80]: "Unauthorized prereleases are unfair to an artist because his or her song is circulating even before it is in its final form. Just as we edit letters and speeches, we must allow songwriters to tweak and refine their works. They deserve to have the tools to penalize those who thrive on the ability to leak a song or CD before it is available in stores or other legitimate avenues of commerce."[81] In a similar vein, during the initial premiere (public release) stage of motion pictures and other works, income potential is at its highest and pirated copies can cause their greatest direct economic harm to the bottom line.[82] This unique status would also argue for rapid notice and takedown of pirated versions of such works.

B. The Author/Subject Dichotomy

As is clear from the New Zealand HDCA, one of the critical distinctions between copyright and privacy focused takedown regimes is the identity of the person whose rights are at issue. Copyright at its heart is focused on the rights of authors, who by definition are the creators of the material sought to be removed. By contrast, those who seek takedowns of "harmful communications," including in particular those that violate personal privacy, are the *subjects* of such materials. With the exception of private works

---

[78] Id. at §512(f).
[79] See generally Jennifer Urban et al, Notice and Takedown In Everyday Practice (March 2017).
[80] 17 U.S.C. § 506(a)(1)(C).
[81] Cong. Record, 109th Congress, 1st Session, Vol. 151, No. 47 at H2118 (April 19, 2005)(Statement of Howard Berman).
[82] See Cong. Record, 109th Congress, 1st Session, Vol. 151, No. 47 at H2118 (April 19, 2005)(Statement of Howard Berman in support of Family Entertainment and Copyright Act of 2005)("Distributing a film before final edits are made can undermine artistic integrity and can also harm the film's commercial prospects because the release is typically coordinated with a marketing effort.").

distributed without authorization, in most cases the individuals seeking takedown do not presently own any copyright interest in such materials. This shift in identity of the protected rights holder does not eliminate the relevancy of privacy considerations. However, it admittedly makes them a secondary factor in NTD reforms, *unless privacy considerations are also used to redefine authorial rights.*

Despite the critical role that authorship plays in the control of rights under copyright, the term is undefined in governing multilateral treaties. With some noted exceptions based on the unique collaborative nature of films and sound recordings,[83] "authors" are generally defined as the human originators of a particular work. Even for countries such as the United States,[84] South Korea,[85] and Japan[86] that recognize non-human authorship in the form of a "work for hire," the entity may be non-human, but the actual creators of the work are still human. In today's digital environment new technologies have created truly potential non-human "authors," including works created by artificial intelligence.

From the copyright ownership of buildings and light displays reproduced in panoramic photos,[87] to the authorship of selfies taken by a monkey,[88] the contours of authorship remains in flux. As countries reconsider the authorial boundaries to be drawn in the face of such new technologies, there is room to reconsider the relationship between the photographer and his subject that lie at the heart of privacy-based copyright norms.[89] Even in cases where the subject has consented to having his photo taken, subjects are increasingly seeking control over the use of those images. In the United States, in *Natkin v. Winfrey*,[90] the well-known celebrity Oprah Winfrey sued for copyright in her images taken by free-lance photographers authorized by her to take such images. The court ultimately rejected the claim because "the subject matter of the photographs is not copyrightable. … To qualify as an author, one must supply more than mere direction or ideas. An author is the party who actually creates the work, that is, the person who translates an idea into a fixed, tangible expression."[91] Neither Winfrey's "facial

---

[83] See, e.g., European Union, Directive on the term of protection of copyright and certain related rights 2006/116/EC (2006), Art.2(1) (establishing that the "principal director" of a cinematographic or audio visual works shall be considered an author)("Copyright Directive"); Australia, Copyright Act § 98 (establishing the "maker" of a cinematographic work as the copyright holder and specifying such "maker" can be the "director" where the film is not a commissioned work); 16 Casa Duse, LLC v. Merkin, 791 F.3d 247 (2d Cir. 2015)(holding producer was author of film).

[84] 17 U.S.C. §201(b).

[85] South Korea, Copyright Act, Art. 9.

[86] Japan, Copyright Act, Art. 15(1).

[87] Doris Estelle Long, World Finds Itself in Quandary Over "Panorama Photos"; Now Come Drones, 161 CHI. DAILY L. BULL. 241 (December 10, 2015);

[88] Complaint, Naruto v. Slater, Case No.: 15-cv-4324 (ND Cal. 2015), available at https://www.animallaw.info/sites/default/files/PETA_%20monkey_selfie%202015.pdf

[89] Susan Corbett, The Case for Joint Ownership of Copyright in Photographs of Identifiable Individuals, 18 Media and Arts Law Review 330-349 (2013).

[90] 111 F.Supp.2d 1003, 1011 (ND Ill. 2000).

[91] Id. at 111 F.Supp.2d at 1011 (citation removed; brackets removed)(Citing *Erickson v Trinity Thirty Theatre, Inc.*, 13 F.3d 1061 at 1071 (7th Cir. 1994), which cited *Community for Creative Non-Violence v. Reid*, 490 U.S. 730, 737 (1989)).

expressions, her attire, the 'look' and 'mood' of the show, the choice of guests [or] the staging of the show"[92] qualified as a copyrightable work.

If privacy issues are considered, at least in cases of unauthorized photography, however, countries might determine that the unwilling subjects have the right to control the future use of their image as, at least, a joint author. Such authorship would not only resolve the issue of the right to control dissemination of private images of sexual conduct, and drone and other forms of unauthorized surveillance images (discussed below), but could also have applications with regard to so-called paparazzi photography, at least where such photographs intrude into the subject's private spaces. One useful example of this approach is New Zealand's grant of a moral right to "[a] person who, for private and domestic purposes, commissions the taking of a photograph or the making of a film" to prevent the public exhibition, communication to the public or issuing of copies, even if the copyright is owned by another.[93] The right of control under this provision would not cover unauthorized photos created by drones or the paparazzi since it is limited to "commissioned" works. But it provides a useful starting place for reconfiguring the rights of photographed subjects (regardless of the medium used to create the image) to prevent the distribution/public communication of hidden photography that is violative of personal privacy.

Given that numerous countries are already considering the lines between authorship and technology, including revisions to the definitions of joint authorship in cases of collaborative works, privacy considerations could rewrite the landscape of such rights. The primary focus on authorship premised on creative contributions could still be maintained. But creative contribution would not need to be constrained to those who knowingly contributed to the work. Instead, privacy considerations could push normative contribution tests so that even unconsented to poses, facial expressions and the like would give rise to sufficient creativity to qualify for joint authorship.[94] Where the unconsented to image violates personal privacy, privacy considerations would argue for the subject having the right to prevent its public distribution/exhibition/communication to the public. Such right to prohibition could be based on an expanded moral right, such as that contained in New Zealand's copyright law, or on a redefined right of control as a joint author.

C. Drones, Surveillance and Data Collections

From drones whose cameras can peek over privacy hedges and into second-story windows, to panoramic drones that create beautiful cinematography, the advance of drone technology has raised the connections between copyright and privacy to new levels of concern. While drones can be used for diverse purposes, including as machines to

---

[92] Id.

[93] New Zealand, Copyright Act of 1994, §105 (as amended by the New Technologies Amendment of 2008 (Section 62(1)).

[94] See Susan Corbett, The Case for Joint Ownership of Copyright in Photographs of Identifiable Individuals, 18 Media and Arts Law Review 330-349 (2013).

transport balloons in parades,[95] their use as aerial camera platforms also invite paparazzi, nosy neighbors and law enforcement to take invasive photos and post them before the subject knows he has been under observation.

Combined with new biometric identification techniques, drone photography eliminates the anonymity crowds or personal property fences might otherwise provide. Yet the current focus on regulating drones as aerial devices by the United States, the European Union and diverse Asia Pacific countries often ignores the reality of their use for civil surveillance. To the contrary, present regulations largely focus on the control of air space above 400 feet, and have relatively few have provisions regarding personal privacy. One notable exception is an ordinance specifically enacted in 2015 by the City of Chicago, Illinois, to address, among other issues, the threat to privacy posed by unregulated civilian drone activity. The Preamble expressly recognized: "Drones can be equipped with highly sophisticated surveillance technology that threatens privacy."[96]

To combat this threat the ordinance provides that no one "shall operate …any small unmanned aircraft in city airspace…. for the purpose of conducting surveillance, unless expressly permitted by law."[97] It further provides an expanded definition of "surveillance" designed to reach all potential intrusions:

> "Surveillance" means the gathering, without permission and in a manner that is offensive to a reasonable person, of visual images, physical impressions, sound recordings, data or other information involving the private, personal, business or familial activities of another person, business or entity, or that otherwise intrudes upon the privacy, solitude or seclusion of another person, business or entity, *regardless of whether a physical trespass onto real property* owned, leased or otherwise lawfully occupied by such other person, business or other entity, *or into the airspace above real property* owned, leased or otherwise lawfully occupied by such other person, business or other entity, occurs in connection with such surveillance.[98]

The Ordinance also prohibits operating small unmanned aircraft "directly over any person who is not involved in the operation of the small unmanned aircraft, without such person's consent;"[99] or "over property that the operator does not own, without the property owner's consent, and subject to any restrictions that the property owner may place on such operation."[100] A "small unmanned aircraft" is defined as "an aircraft that (1) is operated without the possibility of direct human intervention from within or on the aircraft, and (2) weighs less than 55 pounds at the time of the operation, including the

---

[95] Jordan Crook, Disney Files Patents to Use Drones in Park Shows (August 27, 2014), available at http://techcrunch.com/2014/08/27/disney-files-patents-to-use-drones-in-park-shows.
[96] Chicago Ordinance, Preamble, Paragraph.11, available at http://uavs.insct.org/local-regulation
[97] Id. at Art. 1036-400 (b)(12).
[98] Id. at Art. 1036-400 (a)(emphasis added).
[99] Id at Art. 1036-400(b)(2).
[100] Id. at Art. 1036-400(b)(3).

weight of any payload or fuel."[101] Gliders and small aircraft tethered by a wire or rope are expressly excluded from the Ordinance.[102]

New Zealand has created a similar Aviation Rule, requiring persons operating a "remotely operated aircraft" to "avoid operating in airspace above persons who have not given consent for the aircraft to operate in that airspace; and above property unless prior consent has been obtained from any persons occupying that property or the property owner."[103] Similar to the US ordinance, the Rule defines the covered aircraft as "radio controlled" ones and excludes "model aircraft" and "free flight aircraft."[104]

Although Chicago's Ordinance and New Zealand's Aviation Rule prohibits unauthorized flights over people and property, similar to other civilian drone regulations that include privacy concerns within their scope,[105] they do not provide remedies if the results of an authorized overflight are posted on the internet or otherwise published. Some countries may provide some, but not complete relief, under privacy or related laws.[106] Fortunately, the outputs of drones and other surveillance technologies include photographic images and audio recordings that are potentially regulatable under copyright regimes. Thus, their takedown might be possible under a reformed NTD regime discussed above,[107] applying the same normative principles for removal of photographic images that invade personal privacy. Where the invasive materials consist of audio recordings, the normative rules would be different. Assuming that the recorded sounds consist of words, and not just ambient sounds, there is little doubt that such recordings by a drone could be copyright protectable. But there would be less need to reconfigure creativity or authorship norms per se. Instead, the recording by drones could be considered merely a mechanical act, recording without creative input, so that the owner/operator of the drone would have no authorship rights. Instead, the speakers would be the authors of any captured recording.[108]

D. Fair Use, Fair Dealing and the Public Interest in Privacy

Fair use/fair dealing considerations based on unauthorized uses of copyrighted works represents the most obvious normative alteration that inclusion of privacy considerations would present. Privacy considerations have already begun to be recognized as a viable third party interest to be protected against overzealous protection of copyrighted works in

---

[101] Id. at Art. 1036-400(a).

[102] Id. at Art. 1036-400(a). Penalties for violating the Ordinance include fines from $500.00 to $5,000.00 for each offense, and/or incarceration for a term not to exceed 180 days. Id. at Art. 1036-400(d).

[103] New Zealand, Civil Aviation Rule 101.207 (2015)("Aviation Rule")..

[104] Id at Aviation Rule 101.1.

[105] See European Aviation Safety Agency, 'Prototype' Commission Regulation on Unmanned Aircraft Operations (August 22, 2016), available at https://www.easa.europa.eu/system/files/dfu/UAS%20Prototype%20Regulation%20final.pdf.

[106] See HDCA, § 24(2)(allowing quick takedown of images that "cause serious emotional distress.") _; Parliament of the Commonwealth of Australia, Eyes in the Sky, ¶4.15 note10 (detailing state laws governing surveillance that might to used to challenge such images).

[107] See supra Part 3B.

[108] In the United States, the present obligation that a work be "fixed" to qualify for copyright protection, and that such fixation is "by or under the authority of the author;" 17 U.S.C.§§101, 102; would need to be altered for this result to apply.

the heightened scrutiny applied to requests for end user identity subpoenas[109] and to efforts applied to combat pirated works on the internet.[110] However, in the context of fair use/fair dealing considerations, privacy concerns might militate *against* the application of such exceptions, particularly where the underlying work at issue also breaches certain privacy rights. In such cases, privacy concerns would not be the sole factor in determining whether any particular work qualified for an exception under copyright. To the contrary, other factors currently considered in determining whether a particular use is fair, including categorical exceptions for such diverse categories as satire or parody, research, scholarship, current news, security testing and the like, would remain critical factors. But privacy interests would represent a strong "thumb" on the copyright fair use/fair dealing balance. The strength of this factor could be balanced by the same types of considerations that currently regulate the protections given personal data.

We already have examples in numerous regimes aimed at protecting personal data privacy in which special categories of information have been granted heightened protection. For example, under Article 8 of the EU Directive on Data Privacy, sensitive personal information relating to the following categories are subject to extremely narrow processing rights:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade-union membership,
- data concerning health or sex life, and
- data relating to offenses, or criminal convictions.[111]

Article 9 of the European Union General Data Protection Regulation provides greater detail about these protected data categories and includes genetic data, biometric data for the purpose of uniquely identifying a natural person and sexual orientation. [112] Other countries in the Asia Pacific that provide heightened protection for "personal sensitive information" have included additional categories, reflecting expanded norms for such protection. For example, Australia includes "membership of a political association," sexual orientation or practices and biometric templates.[113] Japan includes a crime victim's history and contains a catch-all category "other sensitive information that may

---

[109] See Sony Music Entertainment Inc. v. Does 1-40, 326 F.Supp.2d 556, 564-65 (2d Cir. 2004)(requires evaluation of the "concrete[ness of the plaintiff's] showing of a prima facie claim of actionable harm," consideration of "alternative means" to secure the requested identity disclosure and an express evaluation of the objecting party's expectation of privacy) ; BMG Canada, Inc. v John Doe, 2004 Fed. Ct. Trial Lexis (Federal Ct. Canada 2004)(similar requirements for disclosure); Promusicae v. Telefonica de Espana SAU (Case C275/06)(2008)(similar requirements for disclosure).

[110] See Promusicae v Telefonica de Espana SAU (Case C275/06) ¶70 (2008) ("[Relevant] Directives …do not require the Member States to lay down … an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings.").

[111] European Union, Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 95/46/EC, Art. 8 ("Data Privacy Directive").

[112] GDPR, Art. 9.

[113] Australia, Federal Privacy Act, Art. 6(1).

lead to social discrimination or disadvantage."[114] The Philippines includes "age" and "philosophical affiliations" and expands sensitive information regarding "offenses" to specifically include those that have only been "alleged."[115]

While personal data privacy in these instances focuses on categories of *data* for heightened protection, the California State "Online Eraser" Statute establishes a protected class of *subjects* entitled to greater protection. Chapter 22.1(a) of the California Business and Professions Code obligates the OSP of a site or application "directed to minors" or who has "actual knowledge" that a minor is using its services to remove content posted by the minor *on the minor's request*.[116] A minor is defined as any California resident under the age of 18.[117] There is no obligation that such content be created by the minor or that such content breach the minor's privacy or otherwise cause any type of embarrassment or emotional harm. To the contrary, the purpose for the Online Eraser Statute is to allow those who are underage to remove whatever they might have posted that they now regret for whatever reason. The removal right is not an absolute one. It does not obligate the OSP to remove copies of the posting that appear on other websites. But it does recognize that minors should be subject to special protections given their age and general immaturity of judgment regarding personal privacy boundaries.

These nuanced considerations could be added into an expanded fair use/fair dealing balance that considers the public interest, including the public interest in privacy. Thus, for example, where the original work is an unauthorized image of a minor engaged in sexual activity, the heightened interest in protecting minors against the embarrassment and harm that such privacy violations could cause might well argue against any fair use.

Privacy considerations could also alter the balance in the ability to use unpublished, private works under a fair use/fair dealing exception. Privacy considerations do not necessarily prohibit fair use accommodations for the use of unpublished works. But they do suggest that, just as the nature of the data at issue receives variable protection under privacy regimes, the nature of the work under fair use should be considered. Where that nature is "private" in sense that it has not been published or otherwise distributed or communicated publicly, or where it deals with subject matter of an extremely private personal nature (perhaps as represented by the categories of sensitive data contained in data privacy collection laws discussed above), then personal privacy issues should be given greater consideration.

For those countries with strong moral rights that include the right of divulgation (first publication), such as France,[118] or some variation such as New Zealand's special

---

[114] Japan, Act on the Protection of Personal Information and Amendments, Art. 2(3).
[115] Philippines, Privacy Act, Art. 1(l).
[116] California Business Code, Chap. 22.1, §22581.
[117] Id. at § 22580 (f)
[118] France, Intellectual Property Code, Art. L-121-2 ("The author alone has the right to disclose his work."); Taiwan, Copyright Ordinance, Art 15 ("The author shall enjoy the right to publicly release the work …").

moral rights for photographs,[119] unpublished works are already prevented from unauthorized publication. However, since the right of divulgation is not included in the obligatory moral rights protections under the Berne Convention,[120] such protection is not required. Indeed for countries such as the United States, this right may not even be protectable under the relatively flexible "balancing test" for fair use utilized by the United States,[121] the Philippines,[122] Taiwan,[123] and South Korea,[124] among others.

The United States fair use provision has provided the template for the fair use balancing test internationally. Under this balancing test, the question of whether any use is considered a "fair" one under copyright is determined by balancing four statutory factors. They are:

- The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- The *nature of the copyrighted* work;
- The amount and substantiality of the portion used in relation to the copyrighted work as a whole;
- The effect of the use upon the potential market for, or value of, the copyrighted work.[125]

Although the "nature" of the work is considered, presently such consideration is generally limited to the factual nature of the work. Where a work is considered more factual in nature, such as directories, software codes and the like, an end user can use a greater portion of it and still have such use qualify as a fair one. By adding privacy as a consideration in fair use determinations, the nature of the work would go beyond a simple question of whether the work was more fictive or factual in nature. It would also consider the personal nature of the work and any indicia of the author's desire for its continued secrecy. Like other factors, the unpublished nature of the work or its private or unconsented nature, would not be an absolute bar to a fair use/fair dealing exception. But such private nature would not be given such short shrift as it receives currently in some countries, including the United States.[126] Although including privacy considerations would not automatically lead to a finding against fair use it would at least require more than outright dismissal of an author's interest in maintaining such privacy. For those countries that utilize a fair dealing approach, care in assuring that categories of acceptable uses do not implicitly permit the use of private works, in publication status or its private subject matter, should achieve the same result.

---

[119] New Zealand, Copyright Act, §105.
[120] Berne Convention, Art. 6bis (limiting obligatory moral rights to integrity and patrimony).
[121] 17 U.S.C. §107. See Swatch Group Management Services Ltd. v. Bloomberg L.P., 756 F.3d 73 (2d Cir. 2014)(injunction denied to halt distribution of private recording due to public interest in access to financial information).
[122] Philippines, Copyright Act, Art. 185.
[123] Taiwan, Copyright Act, Art. 65.
[124] South Korea, Copyright Act, Art. 35ter(2).
[125] 17 U.S.C.§ 107 (emphasis added).
[126] Id. (The private unpublished nature of the work "shall not itself bar a finding of fair use").

The normative inclusion of the private nature of the subject matter at issue in a case of fair use or fair dealing would represent a contrary trend toward the current international push to secure greater flexibility in the rights of the public to utilize others' works. This trend is strongly represented by the current trend in the United States to recognize fair use for "transformative" uses that have included the unauthorized digitization of copyrighted works.[127] Including privacy considerations as part of a fair use/fair dealing norm, however, would assure that determinations reflect a careful balance between public access to information and personal dignity represented by increased protection against unauthorized uses that implicate sensitive private information.

E. Resolving the TPM Debate: Considerations of Personal Data Privacy in Access Debates

Since the earliest days of digital media, content owners have attempted to shield their copyrighted works from unauthorized uses through technology. From debates over the requirements of copy controls on digital audio players to the present arms race in encryption and other technologies to prevent unauthorized access, technology has always been perceived, rightly or wrongly, as a potential solution to digital piracy.[128] Even the first multilateral treaty to deal with copyright protection in the Digital Age, the WIPO Copyright Treaty (WCT), set forth a positive obligation on signatories to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights."[129] This obligation has been reiterated in all subsequent WIPO-Administered Treaties dealing with copyrighted content.[130]

The protection of technological protection measures (TPMs) remains a contested issue. Two major areas of contention are the scope of rights to be protected by such TPMs and the application of fair use/fair dealing exceptions to circumvent such measures. Consideration of privacy issues could significantly alter the analysis in both areas.

As noted above, under Article 11 of the WCT, only TPMs erected to protect "the exercise of [author's] *rights*" are covered. This language undeniably includes encryption and other technological measures designed to prohibit unauthorized reproduction or performance of a streamed or downloaded work. It does not, however, mandate protection of TPMs that restrict *access* to copyrighted works. Copyright owners are not granted the express right to prohibit "access" to their works under either international or domestic regimes. Such right of access implies a right to prohibit the "use" of a work. But such "use" right is not, per se, a recognized one under copyright.[131] To the contrary, if a

---

[127] Author's Guild v. Google, Inc., 804 F.3d 202 (2d Cir. 2015).
[128] Add cite to Susan's Chapter
[129] WCT, Art. 11.
[130] WPPT, Art. 18; AVPT; Art. 15.
[131] Doris Estelle Long, *When Worlds Collide: The Uneasy Convergence of Creativity and Innovation,* 25 J. Marshall J. Computer & Info.L. 653 (2009).

work is publicly available, the copyright owner cannot lawfully stop an end user from reading a lawfully acquired copy of the work, or from using the *information* in that work.

In Article 6 of the EU's InfoSoc Directive, protected technological measures were defined as "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or *any right related to copyright as provided for by law* or the sui generis right provided for in the [Database Protection Directive.]."[132] Similar to the language of Article 11 of the WCT, access or use rights are not included among the rights expressly protected under these measures. Section 226(a) of New Zealand's Copyright Act similarly defines a technological protection measure as "any process, treatment, mechanism, device, or system that in the normal course of its operation prevents or inhibits *the infringement of copyright* in a TPM work."[133] China also prohibits the intentional circumvention of TPMs "adopted by a copyright owner … to protect the copyright or the rights related to the copyright in the work to protect the copyright."[134] The rights defined under New Zealand's copyright laws do not include "access" or "use" rights.[135] Neither do those under China's copyright laws.[136]

By contrast, section 1201of the United States DMCA expressly prohibits the circumvention of technological protection measures designed to "control access" to a copyrighted work[137] or to protect "a *right* of a copyright owner."[138] Several Asian Pacific countries provide for similar protection for access control measures, including Australia,[139] Singapore,[140] South Korea[141] and Taiwan.[142] The United States, however, provides potentially the strongest protection for such access measures because it rejects any fair use exceptions to permit circumvention of access protection TPMs. Section 1201(a)(1)(A) expressly provides "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[143] As the US Copyright Office recognized in its Executive Summary of the DMCA: "[S]ince the fair use doctrine is not a defense to the act of gaining unauthorized access to a work, the act

---

[132] European Union, Info Soc. Directive, Art. 6 (emphasis added).
[133] New Zealand, Copyright Act, § 226(a)(emphasis added). But see New Zealand TransPacific Partnership Amendment Act 2016 § 226AC (establishing anticircumvention protection for an "access control TPM"). The Amendment does not come into force until the TransPacific Partnership comes into force in New Zealand. Id. at § 44. Insert citation to Susan's Chapter here.
[134] PRC, Copyright Act, Art. 48(6).
[135] New Zealand, Copyright Act, §§ 29 - 39.
[136] PRC, Copyright Act, Arts. 10 & 48.
[137] 17 USC § 1201(a).
[138] Id. at § 1201(b).
[139] Australia, Copyright Act § 116AN.
[140] Singapore, Copyright Act, Art. 261B.
[141] South Korea, Copyright Act, Art. 2(28).
[142] Taiwan, Copyright Act, Art. 80ter. For a discussion of the potential expansion to protection for access control TPMs in New Zealand, see insert Susan's chapter here.
[143] 17 U.S.C. § 1201(a)(1)(A). See also Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

of circumventing a technological measure in order to gain access is prohibited." [144] The ultimate impact of this distinction was to make protection for access restrictive measures stronger than those for rights-restrictive ones.[145]

One of the sharpest debates to date remains the balance to be struck between protection of technological measures to reduce piracy and access rights, particularly those supported by fair use/fair dealing considerations. Privacy considerations would undoubtedly impact the normative balance struck between protection and access. Similar to its impact on other fair use/fair dealings discussed above,[146] privacy considerations could have a strong impact on the categories of materials to be *excluded* from any fair use exceptions to circumvention controls. For instance, greater protection for TPMs might be desirable where they are used to protect copyrighted works that also pose serious privacy threats if breached. For the same reason, however, privacy issues might resurrect the desirability of expanding protected TPMs from rights-based to access-restrictive ones at least for certain types of private information whose dissemination should remain in the hands of the copyright owner.

The normative inclusion of the private nature of the subject matter at issue with regard to technological protection measures would represent a contrary trend toward the current international push to secure greater flexibility in the rights of the public to access TPM-protected works in certain cases. But it could also be used to draw a clearer normative line between works that are deserving of heightened protection (because of their sensitive subject matter) and those for which fair use/fair dealing rights should be allowed. Such addition, however, would not fully answer the issue of how to secure fair use/fair dealing access while maintaining anti-circumvention measures as a viable method for protecting copyrighted works. It could, however, provide needed illumination on why this issue still matters.

F. Distributional Controls, Transformations and Injunctive Relief

As noted above, privacy considerations could significantly alter the normative scope of notice and takedown processes designed to assist in the protection of copyright interests in the Digital Age.[147] Yet the impact of such considerations on enforcement mechanisms would not be limited solely to this admittedly critical issue. To the contrary, adding privacy issues into normative reforms in copyright could directly impact critical questions regarding the scope of relief available for infringing uses. In short, it could impact the extent to which copyright owners would be entitled to injunctions against the continued unauthorized use of copyrighted materials.

One of the most consistent debates over the scope of protection afforded copyrighted works is whether such works represent property rights for which injunctive

---

[144] The Digital Millennium Copyright Act: U.S. Copyright Office Summary (Dec. 1998).

[145] *The Chamberlain Group, Inc. v. Skylink Technologies, Inc*, 381 F.3d 1178, 1201 (Fed. Cir. 2004)(holding that only access- restrictive TPMs that "bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners" fell within the scope of Section 1201 protections).

[146] See Discussion supra Part 3A.

[147] See Discussion supra Part 3D.

relief against unauthorized uses should be available or whether liability rules that impose money damages are sufficient.[148] Even in the United States, injunctive relief is no longer always granted in cases of copyright infringement. Instead, courts examine whether irreparable harm will occur to the copyright owner.[149] Historically, such harm was presumed to occur. Currently, courts not only require that copyright owners "show that, on the facts of their case, the failure to issue an injunction would actually cause irreparable harm."[150] Courts must also consider the public interest:

> The object of copyright law is to promote the store of knowledge available to the public. But to the extent it accomplishes this end by providing individuals a financial incentive to contribute to the store of knowledge, the public's interest may well be already accounted for by the plaintiff's interest. The public's interest in free expression, however, is significant and is distinct from the parties' speech interests. ...Every injunction issued before a final adjudication on the merits risks enjoining speech protected by the First Amendment.[151]

If privacy considerations were added into the irreparable harm/public interest balance, depending on the subject matter of the work at issue, injunctive relief might become more readily available. "Liability rules" that favor the imposition of what amounts to a compulsory license for the use of the infringed work might be preferable where a work has a non-speculative commercial value that can be readily calculated. But if the work also poses a serious threat to the public's interest in personal privacy, such compulsory licenses would be wholly inappropriate. For example, the public interest in limiting the harm caused by the dissemination of works that qualify as sexting or revenge porn would support injunctions against their further distribution.

Alternatively, depending on their subject matter, privacy considerations could well be used to deny enforcement to the holders of copyright in such works. Many countries, including the United States refuse to enforce copyright in works that are considered obscene or pornographic.[152] Similar denials of enforcement could be extended to works such as surveillance videos or depictions of private sexual activity that represent a serious violation of personal privacy rights. At its most extreme, revised copyright norms might even deny subject matter eligibility to works that present the greatest threat to personal privacy.

---

[148] See Tracy Lewis & J.H. Reichman, "Using Compensatory Liability Rules to Stimulate Innovation in Developing Countries," in International Public Goods And Transfer Of Technology Under A Globalized Intellectual Property Regime (Keith Maskus & J.H. Reichman eds. Cambridge Univ. Press) (2005).
[149] See *Ebay Inc. v. MercExchange LLC,* 547 US 388, 392-393 (2006)("This Court has consistently rejected invitations to replace traditional equitable considerations with a rule that an injunction automatically follows a determination that a copyright has been infringed.").
[150] Salinger, v. Colting, 607 F.3d 68, 82 (2d, Cir. 2010).
[151] Id. at 607 F.3d at 82.
[152] Devil's Films Inc. v. Nectar Video, 29 F.Supp.2d 17 (S.D.N.Y. 1998).

Adoption of enforcement norms that decline enforcement on the grounds of the private nature of the materials could serve as a useful adjunct to other normative protections discussed previously. At a minimum, they would prevent aggressive cyberbullies and revenge porn posters from securing relief under declaratory relief actions when their posts are challenged. But these provisions are only supplementary and should not take the place of NTDs and other methods for reforming copyright to protect personal privacy.

Conclusion

The rapid change in technology over the past several decades has rewritten the practical realities of the role of copyright in today's global digital environment. As countries struggle to reform present norms, derived largely from an older hard-goods-focused world, new inputs are needed to assure that the reconfigured regimes created today accurately reflect present realities and future possibilities. Among those "new" inputs should be a consideration of the inter-relationship between copyright and personal and data privacy.

There has always been a tangential relationship between copyright and personal privacy regimes in connection with identity disclosures of potential infringers. Yet over time, this relatively slight relationship has expanded to the point where privacy considerations are beginning to influence international copyright norms. Such considerations have already begun to change the boundaries of authorial rights in the 21st Century. Their formal inclusion as part of the normative background for present efforts at copyright reform is long overdue and could add clarity and even new paradigms for the future. Privacy norms have the possibility of significantly changing present copyright norms by adding new issues and new points of view.

Yet simply adding privacy issues into the copyright reform "mix" and adopting some of the norms discussed in this Chapter is only the first step in creating a normative framework for copyright that avoids the empty promises of the 1990s. To create copyright laws that will survive the next technological revolution, we must create a harmonized reformation, a code that will assure that these critical normative changes are incorporated across borders. Merely creating a patchwork of reformed laws in some countries based on new privacy-informed regimes may be better than making no change at all, but it disserves the borderless realities of the digital environment. Fortunately, the task is made easier in the Asia Pacific because a draft Copyright Code for the region has already been created by Professor Adrian Sterling.[153] This Code provides the critical framework of foundational norms that could be examined and potentially strengthened through a reconsideration of the current separation between copyright and privacy laws. If we truly want to create copyright laws for the 21st Century, we must be brave enough to complete the entire task. Anything less will simply leave the work for another generation. Given how quickly technology moves, I am not certain we can wait that long.

---

[153] Adrian Sterling, Draft Asia Pacific Copyright Code (2015), available at http://www.apcacopyright.org/conference-2015/conferences/copy-right-law-and-policy-in-the-asia-pacific-conference-2015. See note 8 and accompanying text supra.