No Country for Cybersecurity Arbitrage

Eli Greenbaum*

Introduction

On October 28, 2016, regulations issued by the Copyright Office exempted a wide swath of cybersecurity research from the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA).[1] These regulatory exemptions were motivated by assertions that the DMCA anti-circumvention prohibitions hinder cybersecurity research and practice. This article investigates the accuracy of these claims by examining the single developed market economy[2] that does not prohibit (and is not obligated under treaty to prohibit) the use of anti-circumvention technology. More generally, this article examines the ability of firms to engage in international regulatory arbitrage – to exploit regulatory disparities across jurisdiction.[3] The analysis demonstrates that opportunities to engage in regulatory arbitrage cannot be analyzed without attention to the identity and structure of industry players.

Broadly speaking, anti-circumvention prohibitions assist copyright holders in controlling their works. Copyright holders often use technology to prevent unauthorized use or distribution. Such technology may include, for example, measures that prevent the illicit distribution of music or e-books, software that prevents the use of mobile phones on competing networks,[4] or mechanisms that prevent unauthorized tampering with software in automotive vehicles.[5] Statutory anti-circumvention prohibitions (such as those in the DMCA) impose civil or criminal liability for bypassing such technological measures.

Over the last twenty years, international treaties have required most of the developed world to ban technology that circumvents technological protection measures. Israel is unique among the developed market economies in that it has not, and vociferously does not intend to, promulgate any anti-circumvention prohibitions. In superficial confirmation of the cybersecurity criticisms of anti-circumvention law, Israel boasts a booming industry in security technology, far out

---

* Partner, Yigal Arnon & Co., Jerusalem, Israel. J.D., Yale Law School; M.S., Columbia University.

[1] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944 (Oct. 28, 2015) (to be codified at 37 C.F.R. pt. 201) [hereinafter *2015 Exemptions*]. Most provisions of the 2015 Exemptions came into effect on October 28, 2015. The effectiveness of the security research exemption was delayed for one year in order to allow "other parts of the government sufficient opportunity" to opine on the "wisdom of granting an exemption" for the purpose of cybersecurity research. *Id.* at 65,956.

[2] This Article uses a country's membership in the Organization of Economic Cooperation and Development ("OECD") as a proxy for whether it constitutes a developed market economy.

[3] For a description of how intellectual property rules may enable international regulatory arbitrage, *see* Pamela Samuelson, *Intellectual Property Arbitrage: How Foreign Rules Can Affect Domestic Protections*, 71 U. CHI. L. REV. 223 (2004).

[4] *See, e.g.,* Tracfone Wireless Inc. v. Dixon, 475 F. Supp. 2d 1236 (M.D. Fla. 2007) (holding that unlocking cellular handsets violates the DMCA).

[5] *See* 2015 Exemption, *supra* note 1, at 65,954 (discussing anti-circumvention technology in motor vehicles).

of proportion to its relatively small population. Nevertheless, as shown below, there is scant evidence to connect Israel's success in cybersecurity to its lack of anti-circumvention prohibitions.

This article complements existing literature by providing insight into the actual effects of non-circumvention prohibitions, and the current wisdom of creating a regulatory exception for security research. In a broader sense, however, the paper adds to a "surprisingly thin"[6] literature on international regulatory arbitrage. Existing research into regulatory arbitrage has mostly concentrated on how jurisdictions compete for business activity through regulatory innovation, with little attention paid to how actors and institutions actually take advantage of those differences or how arbitrage opportunities are mediated by technological, commercial and national institutions.[7] This paper shows the importance of analyzing the character and organization of firms and institutions in determining the scope of actual arbitrage opportunities.

I. Anti-Circumvention and Security Research

Anti-circumvention restrictions have been imposed by many countries, and are cemented in international treaties. Article 11 of the WIPO Copyright Treaty (WCT), for example, provides that countries will protect "against the circumvention of effective technological measures . . . that restrict acts, in respect of their works, which are not authorized by the authors."[8]

In 1998, Congress passed the DMCA, bringing the United States into compliance with the WCT. The DMCA prohibits circumvention of any "technological measure that effectively controls access" to a copyrighted work.[9] In addition, the DMCA prohibits trafficking in technology that is designed or marketed for the purpose of circumventing protection measures that control access to or copying of copyrighted works.[10] The European Union implemented the anti-circumvention provisions of the WCT treaty in EU Directive 2001/29/EC. The Directive requires member states to provide "adequate legal protection against the circumvention of any effective technological measures" as well as against the trafficking of circumvention technologies.[11]

A number of commentators have expressed strong concern that anti-circumvention prohibitions discourage research into security vulnerabilities.[12] In the course of investigating any specif-

---

[6] Annelise Riles, *Managing Regulatory Arbitrage: A Conflict of Laws Approach*, 47 CORNELL INT'L L.J. 63, 68 (2014).

[7] Claudio M. Radaelli, *The Puzzle of Regulatory Competition*, 24 J. PUB. POL'Y 1, 13 (2004) (stating that "we do not know enough about how corporations … respond to international regulatory competition").

[8] World Intellectual Property Organization Copyright Treaty art. 11, Dec. 20, 1996, 17 U.S.C. §§ 1201–1205. Article 18 of the World Intellectual Property Organization Performance and Phonograms Treaty contains a similar provision. *See* World Intellectual Property Organization Performances and Phonograms Treaty art. 18, December 20, 1996, 17 U.S.C. §§ 1201–1205.

[9] 17 U.S.C. § 1201(a)(1) (2016).

[10] 17 U.S.C. § 1201(a)(2) (2016) (prohibition on trafficking in technology that circumvents access controls); 17 U.S.C. § 1201(b)(1) (2016) (prohibition on trafficking in technology that circumvents the "protection afforded by a technological measure that effectively protects a right of a copyright owner").

[11] EU Directive 2001/29, art. 6, 2001 O.J. (L 167) 17 (EC) [hereinafter *EU Copyright Directive*]. Council Directive 91/250, 1991 O.J. (L 122) (EC) also imposes anti-circumvention prohibitions on software works.

[12] *See, e.g.*, Derek E. Bambauer and Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051 (2011); Jennifer Stisa

ic technology for vulnerabilities, security researchers are likely to probe and possibly disable any technical measures protecting such technology. Moreover, the subsequent dissemination and publication of such security research – which can include directions on how to circumvent the protection measure – could lead to charges of illegal "trafficking" in circumvention technology. Indeed, individuals conducting research into security vulnerabilities have been threatened with civil and criminal action under the anti-circumvention provisions of the DMCA.[13]

The DMCA does contain statutory exceptions permitting "encryption research"[14] and "security testing"[15] activities. These statutory exceptions, however, are limited by an array of conditions that narrow their practical significance.[16] Exemptions for security and encryption research in the EU Directive are also limited. Recital 48 of the Directive does declare that the anti-circumvention prohibition "should not hinder cryptography research," but this declaration was not translated into an operational provision of the Directive. Only a limited number of EU countries have in fact implemented any exceptions for encryption research or security activities in their national laws.[17]

The DMCA authorizes the Librarian of Congress to grant limited exemptions to the DMCA anti-circumvention prohibitions.[18] Given the narrow applicability of the statutory exceptions, interested parties have over the years applied to the Librarian to obtain broader exceptions for security research activities. After overcoming its initial skepticism, the Librarian granted a number of relatively narrow exceptions for security testing.[19] In the recent 2015 rulemaking, however, the Librarian granted the broadest exception to date for "good faith security research."[20] This last exception was granted pursuant to findings that the existing statutory exceptions were "inadequate to accommodate" security research activities "due to various limitations and conditions", and that the anti-circumvention prohibitions of the DMCA had hindered "legitimate security re-

---

Granick, *The Price of Restricting Vulnerability Publications*, 9 INT'L J. COMM. L. & POL'Y 1, 9 (2005); Joseph P. Liu, *The Law and Technology of Digital Rights Management: The DMCA and the Regulation of Scientific Research*, 18 BERK. TECH. L.J. 501 (2003).

[13] Bamberger & Day, *supra* note 12, at 1080; Granick, *supra* note 12, at 10, 19. The Librarian of Congress expressed similar concerns when promulgating the 2015 Exemptions. *See infra* text accompanying note 21.

[14] 17 U.S.C. § 1201(g) (2016).

[15] 17 U.S.C. § 1201(j) (2016).

[16] Bambauer & Day, *supra* note 12, at 1083; Liu, *supra* note 12, at 509.

[17] Ian Brown, *The Evolution of Anti-Circumvention Law*, 20 INT'L REV. L. & COMPUTERS 240 (2006).

[18] 17 U.S.C. §§ 1201(a)(1)(B)–(D) (2016).

[19] The first request for security testing exemptions was advanced during the 2003 rulemaking procedures, but the Librarian asserted that the request "failed to explain why the existing exemptions are insufficient." Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 68 Fed. Reg. 62,011, 62,018 (Oct. 31, 2003). During the 2006 rulemaking process, the Librarian granted a narrow exception for security research in CDs, finding the exception necessary "in light of . . .[the] uncertainty" of the statutory exception "and the seriousness of the problem" of security vulnerabilities. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,477 (Nov. 27, 2006). The 2010 rules contained an exception for the circumvention of technical protection measures applicable to video game technology. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 75 Fed. Reg. 43,825, 43,839 (July 27, 2010).

[20] 2015 Exemptions, *supra* note 1, at 65,956.

search."[21] Even this relatively broad exemption, however, were circumscribed by a number of limitations and restrictions.[22]

II. A Regulatory Arbitrage Opportunity

Alone among the OECD countries, Israel has neither implemented any anti-circumvention prohibitions in its domestic law nor is it under any international treaty obligation to implement such prohibitions.[23] Indeed, the legality of circumventing technological protection measures in Israel is unusually clear.[24] In 2007 Israel adopted a new copyright law, which deliberately omitted any provisions concerning anti-circumvention technology. As described in more detail below, The Supreme Court of Israel subsequently confirmed that Israeli copyright law cannot be interpreted to infer a prohibition on anti-circumvention technology. Moreover, also as described below, Israel has defended its lack of legal anti-circumvention prohibitions on the international stage.

In 2013, the Supreme Court of Israel confirmed in *Telran Communications (1986), Ltd. v. Charlton, Ltd.* that Israeli copyright law, in the absence of any express provisions prohibiting the circumvention of technological measures, could not be interpreted to imply such a prohibition.[25] The *Telran* defendants sold (unauthorized) cards that allowed for the decryption of foreign satellite communications. The plaintiff asserted that Telran's sale of the cards interfered with plaintiff's exclusive rights to broadcast the 2006 World Cup within Israel. The case raised a number of questions, including as to whether the circumvention of broadcast encryption was prohibited by Israeli law. The Court noted that the Knesset was aware of the WCT treaty, and yet did not include prohibitions on circumvention technology in domestic Israeli law. As such, the Court ruled that existing statutory provisions could not be interpreted to prohibit circumvention technologies.

Moreover, the government of Israel has publicly defended its failure to implement prohibitions against circumvention measures. Until 2014, Israel was included in the annual Special 301

---

[21] *Id*.
[22] *Id.*
[23] All OECD countries have acceded to the WCT treaty save Iceland, Israel, New Zealand and Norway. For a list of the contracting parties to the WCT, *see WIPO Copyright Treaty Contracting Parties*. WORLD INTELL. PROP. ORG., http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16 (last visited Jan. 21, 2017). Nevertheless, Iceland and Norway, as members of the European Economic Area, have implemented prohibitions on anti-circumvention technology in their domestic law. *See* Copyright Act, Article 50a–50d (Act No. 73/1972)(Ice.); Copyright Act, Sections 50a–50e (Act No. 2/1962)(Nor.). New Zealand has also implemented anti-circumvention provisions in its domestic law. *See* Copyright Act, Sections 226A–226E (Act No. 143/1994)(N.Z.). Chile has to date not implemented any anti-circumvention provisions under its domestic law, though it is obligated to do so under Article 11 of the WCT treaty and Article 17(5) of the United States-Chile Free Trade Agreement. *See* United States-Chile Free Trade Agreement, art. 17(5), June 6, 2003, 19 C.F.R. §§ 10.401–10.490; World Intellectual Property Organization Copyright Treaty art. 11, Dec. 20, 1996, 17 U.S.C. §§ 1201–1205.
[24] The ability to engage in international regulatory arbitrage depends to some extent on the clarity of the regulatory differences between jurisdictions. *See* Radaelli, *supra* note 7, at 7.
[25] CA 5097/11 Telran Communications (1986) Ltd. v. Charlton Ltd (Nevo, September 2, 2013) (Isr.).

Report of the United States Trade Representative (USTR).[26] In each report, the USTR encouraged Israel to implement the WCT treaty (and, by extension, prohibitions on the circumvention of technological measures). Nevertheless, in a 2009 submission to the USTR, the Israeli government boldly refused to implement anti-circumvention prohibitions, noting that several large Israeli "authors' groups" were "vehemently opposed" to such bans.[27]

The case of Israel provides an excellent test case for analyzing claims that legal anti-circumvention restrictions impede security research. If such assertions are correct then, all things being equal, jurisdictions that lack such circumvention prohibitions should see a boost to their cybersecurity research and development efforts.[28] Academics in such jurisdictions would be able to conduct research that would be legally problematic elsewhere. Multinationals would be able to shift cybersecurity research to such countries, evading the legal problems that would dog those efforts in other jurisdictions. Local technologists would gain unique experience in circumvention technologies, and startups benefiting from the unique ecosystem would be able to develop inimitable products and services.

Indeed, Israel boasts a booming cybersecurity industry. Israel, with a population of just more than 8 million, exports more cybersecurity-related products and services than all other countries in the world combined, excluding the United States.[29] Reports show the tiny country making 5% of all global sales in cyber security products and attracting 20% of global investment in the sector.[30] Israel should be exceedingly well positioned to take advantage of any arbitrage opportunity presented by its lack of anti-circumvention prohibitions.

Even so, there is scant evidence to connect Israel's cybersecurity prowess to its lack of legal prohibitions on circumvention technology. Instead, Israel's unusual expertise in cybersecurity is variously attributed to government support of the industry, the country's precarious geopolitical security position, public investments in education, or connections between the Israeli military and civilian technology firms.[31] Scholarly accounts of Israel's cybersecurity policies do not ad-

---

[26] The Special 301 Report is an annual report produced by the USTR reviewing the "global state of intellectual property rights (IPR) protection and enforcement." OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, SPECIAL 301, https://ustr.gov/issue-areas/intellectual-property/Special-301.

[27] OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, 2009 SUBMISSION OF THE GOVERNMENT OF ISRAEL TO THE UNITED STATES TRADE REPRESENTATIVE WITH RESPECT TO THE 2009 "SPECIAL 301 REVIEW", at 8. *See also* Nate Anderson, *Israel Rebukes US: Our Copyright Laws Are Fine, Thanks*, ARS TECHNICA (Mar. 18, 2008), http://arstechnica.com/uncategorized/2008/03/israel-rebukes-us-our-copyright-laws-are-fine-thanks/.

[28] *See* Samuelson, *supra* note 3, at 226 (discussing how lower-protection IP regimes can spur innovation in software).

[29] Barbara Opall-Rome, *Israel Claims Surge in Cyber Sales, Investment*, DEFENSE NEWS (Jan. 21 2016), http://www.defensenews.com/story/defense/2016/01/21/israel-claims-surge-cyber-sales-investment/79119378/.

[30] *See, e.g.*, *id*.; John Reed, *Israel Cyber-Security Expertise Lures Growing Share of Investment*, FINANCIAL TIMES (Jan. 12, 2016), http://www.ft.com/cms/s/0/dfa5c916-b90e-11e5-b151-8e15c9a029fb.html#axzz4DP5aeWoU. For a wide-ranging discussion of Israeli advances in cybersecurity, see MICHAEL EISENSTADT & DAVID POLLOCK, WASHINGTON INSTITUTE FOR NEAR EAST POLICY, ASSET TEST: HOW THE UNITED STATES BENEFITS FROM ITS ALLIANCE WITH ISRAEL 34-37 (2012).

[31] *See, e.g.*, LIOR TABANSKY & ISAAC BEN ISRAEL, CYBERSECURITY IN ISRAEL 18 *et seq.* (2015) (attributing Israel's high-technology success to elements of culture and human capital, including the role of the military in developing these, and government incentives for research and development); Peter Suciu, *Why Israel Dominates in Cyber Secu-*

dress Israel's lack of anti-circumvention prohibitions.[32] Multinationals with Israeli branches do not point to the lack of anti-circumvention prohibitions as a reason for establishing those offices.[33] In sum, an objective outside observer of Israel's cybersecurity industry would be justified in concluding that the country's lack of anti-circumvention prohibitions is irrelevant to the success of its cybersecurity industry.

Exemptions to anti-circumvention prohibitions are not costless. Allowing circumvention activities can, aside from increasing the risk of intellectual property infringement, raise serious security[34] and safety concerns.[35] The case of Israel may show that the benefit to security research from permitting circumvention activities is minimal. As such, the new DMCA regulatory exemptions for security research may not be justified, in that they impose substantial risks for little profit.

III. Structural Barriers to Arbitrage

At first glance, the seemingly underwhelming effects of Israel's regulatory regime suggest that non-circumvention controls have little impact on the cybersecurity industry. This section, however, considers a number of structural barriers that may prevent actors and institutions from exploiting the opportunity presented by Israel's lack of anti-circumvention controls. In other words, the failure of industry and academic players to arbitrage Israel's lack of anti-circumvention prohibitions may not mean that such prohibitions do not impact security research. Rather, the ability of actors to take advantage of international regulatory differences must be evaluated in light of constraints and incentives in the industry.

First, the internal organization of commercial cybersecurity firms may prevent those companies from engaging in cross-border legal arbitrage. Cybersecurity firms often boast international teams, providing such companies with the capability of providing around-the-clock services for malware analysis and software support.[36] Such global firms are often structured to allow cross-border cooperation among international teams and, as such, they may resist arbitrage opportunities that require them to cage specific activities within a single jurisdiction. Smaller, local firms

---

rity, FORTUNE (Sept. 1, 2015), http://fortune.com/2015/09/01/why-israel-dominates-in-cyber-security/ (attributing Israel's success in cybersecurity to geopolitical pressures on the country).

[32] *See, e.g.*, Daniel Benoliel, *Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study*, 16 N.C. J.L. & TECH. 435 (2015).

[33] *See, e.g.*, Einat Paz-Frankel, *Why the World's Largest Tech Companies All Want a Piece of the Israeli Pie*, NOCAMELS ISRAELI INNOVATION NEWS (Sept. 30, 2015), http://nocamels.com/2015/09/multinational-high-tech-companies-presence-israel/.

[34] *See, e.g.*, *2015 Exemptions*, *supra* note 1, at 65,955 (noting concerns that information obtained from circumvention activities could be used to "hack into highly regulated machines and devices, including medical devices and vehicles").

[35] *See id.* (expressing concern that "security researchers may not fully appreciate the potential ramifications of their acts of circumvention on automobile safety").

[36] *See, e.g.*, KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON 19, 58 (2015) (describing international cooperation among teams in the computer security industry).

may also refrain from pursuing activities upon which the global economy looks askance, especially if the local firm is hoping to be acquired by an international cybersecurity concern.

From this perspective, the very uniqueness of Israel's legal position may prevent firms from effectively pursuing the arbitrage opportunity. A global firm that wishes to exploit Israel's exceptional lack of anti-circumvention prohibitions must be careful to confine any potentially illegal circumvention activities to Israel. Employees and contractors located outside Israel must, regardless of how the firm ordinarily structures its international cooperation, shy away from those activities. The firm's legal counsel may have difficulty drawing a precise line between permitted international interaction and proscribed assistance to the "rogue" Israeli researchers. In other words, a firm may determine that the cost of realizing the arbitrage possibility (and disregarding clear, firm-wide standards) exceeds the benefit to be had from the arbitrage itself.[37]

Second, the distinctive structure of anti-circumvention provisions may work to thwart the possibility of legal arbitrage. Many jurisdictions prohibit not only the act of circumvention, but also the act of trafficking in circumvention technologies.[38] These trafficking prohibitions may not legally reach extraterritorial conduct, but in practice they hinder cybersecurity research worldwide. First, researchers may be concerned that scholarship disseminated in other jurisdictions could violate those countries' bans on trafficking in circumvention technologies, even though the research was originally published in jurisdictions where those activities were legal.[39] Second, trafficking prohibitions could limit the enthusiasm of multinationals to take advantage of the arbitrage opportunity, since any cross-border sharing of legally developed circumvention technology could violate the trafficking ban. In other words, the trafficking prohibition makes it more difficult to cage anti-circumvention activities in Israel, thus further limiting the ability of firms to engage in regulatory arbitrage.

A third possibility would view Israel's legal arrangements as less unique than presented by a first reading of the statutory anti-circumvention prohibitions. Commentators have noted that much Israeli cybersecurity research and development occurs in the context of Israel's military and national security organizations. These organizations also serve as training grounds for future technologists and entrepreneurs, many of whom join the commercial sector or establish startup companies when they conclude their military service.

Like Israel, many countries can conduct research into circumvention technologies through their military or other security organizations. Laws against circumvention technology often exempt law enforcement, militaries and security agencies from that prohibition. For example, the DMCA expressly exempts "lawfully authorized investigative, protective, information security, or intelligence activity" from its anti-circumvention prohibitions.[40] This exemption also extends to

---

[37] *Cf.* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 806 (2001) (discussing the difficulty of complying with inconsistent regulations across jurisdictions).
[38] *See supra* notes 10-11 (noting anti-trafficking provisions in the DMCA and European Union Directives).
[39] Foreign computer programmers have in fact been arrested in the United States under the DMCA for their part in creating circumvention technologies abroad. *See* Liu, *supra* note 12, at 514.
[40] 17 U.S.C. 1201(e) (2016).

contractors working on behalf of the government.[41] Similarly, the EU Copyright Directive provides that the anti-circumvention prohibition shall be applied "without prejudice to … public security."[42] As such, Israel's military institutions and actors do not benefit from a unique legal space for circumvention technologies. Rather, experience in circumvention technologies can be had in security agencies worldwide.

IV. Conclusion

Israel's resistance to controls on circumvention technology contrasts starkly with the legal picture in other developed countries, presenting a clear opportunity for international regulatory arbitrage. Industry players, however, seem to have declined the chance to exploit Israel's distinctive legal position, and this article has suggested a number of explanations for their reluctance. The common denominator of these suggestions is that the possibility of regulatory arbitrage cannot be analyzed independently of the character and organization of the institutions that engage in the regulated activity. Commercial entities, and especially multinationals, may not be structured in a manner that facilitates recognition and exploitation of differences across jurisdictions. On the other hand, governments and militaries may not require the possibility of regulatory arbitrage in order to engage in the controlled activity. At base, the analysis of international regulatory arbitrage and competition demands not only the identification of appropriate legal differences, but also an analysis of the structures and incentives that facilitate or prevent the exploitation of those differences.

---

[41] *Id.*

[42] *EU Copyright Directive*, *supra* note 11, at 14. *See also id*. at 18 ("This Directive shall be without prejudice to provisions concerning . . . security.").