ENFORCEABILITY OF ANTI-REVERSE ENGINEERING CLAUSES IN SOFTWARE LICENSING AGREEMENTS: THE CHINESE POSITION AND LESSONS FROM THE UNITED STATES AND EUROPEAN UNION'S LAWS

YANG CHEN*

ABSTRACT

Current laws related to intellectual property (IP) protection, especially those meant for protecting copyrights and trade secrets, afford certain strong protections for software programs. However, all IP laws have their limits set by legislators purposefully, to maintain a sound balance between private monopoly rights and public interest. To deal with these limits, software companies frequently include certain restrictive provisions in software end-user licensing terms. The anti-reverse engineering clause is a typical example of companies' efforts to supplement IP protections for software programs. The enforceability of these terms is a critical issue because they disrupt the balance intended by IP laws. This Article discusses the position of China on the enforceability of anti-reverse engineering clauses and finds that the Chinese position is too uncertain. By drawing on insights and policy considerations from the United States and European Union positions, this Article argues that the one-size-fits-all approach is inadequate for China and that an intermediate approach would be a more appropriate alternative. Specifically, it contends that the Chinese law should be reformed to include clear provisions allowing limited contractual

* 2020-2021 Zhao/Zeng Scholar and SJD candidate, University of Pennsylvania Carey Law School; LLM with distinction, University of Pennsylvania Carey Law School; LLM (Corporate and Commercial Law Specialism), London School of Economics and Political Science; LLB, China University of Political Science and Law; Admitted to PRC Bar; Passed NY Bar. Thanks for comments and advice from Professor Gideon Parchomovsky, Professor Victoria Cundiff and SJD fellow Sin Chit LAI.

bans but disallowing total bans on reverse engineering programs. Moreover, a miscellaneous provision should be included to address the rapid development of this industry and deal with an unpredictable future landscape.

TABLE OF CONTENTS

I. INTRODUCTION

> "You are *not allowed* to copy, modify, distribute, sell, or lease any part of the software, or to *reverse-engineer* or attempt to extract the source code of that software, unless laws prohibit these restrictions or you have YouTube's written permission."
>
> —YouTube Terms of Service[1]

> "You *may not*: . . . make copies, modify, adapt, translate, *reverse engineer, disassemble, decompile* or create any derivative works based on the Services, including any files, tables or documentation (or any portion thereof) or determine or attempt to determine any source code, algorithms, methods or techniques embodied in the Platform or any derivative works thereof *unless* any such activities are expressly authorised by us in advance."
>
> —TikTok Terms of Service[2]

> "(6) the term '*improper means*' — . . . (B) *does not include reverse engineering*, independent derivation, or any other lawful means of acquisition."
>
> —2016 Defend Trade Secrets Act[3]

Twitter, TikTok, Facebook, and YouTube are all examples of application software programs used by millions across the globe on computers or phones. As valuable intangible assets of companies around the world, software programs are unique subject matters for IP protection. They are normally distributed in the form of object code, consisting only of strings of ones and zeros, which may only be read by machines.[4] Object code, however, is transformed from

---

[1] *Terms of Service*, YOUTUBE, https://www.youtube.com/static?template=terms [https://perma.cc/CUK6-ZL5A] (last visited Jan. 25, 2022) (emphasis added).

[2] *Terms of Service, Art. 5, 7*, TIKTOK, https://www.tiktok.com/legal/terms-of-service?lang=en [https://perma.cc/U8K8-N8HV] (last visited Jan. 25, 2022) (first emphasis added).

[3] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 2(b)(6)(B), 130 Stat. 376, 381 (emphasis added).

[4] Scott Wallask, *source code*, TECHTARGET (updated Sept. 2019), https://searchapparchitecture.techtarget.com/definition/source-code [https://perma.cc/GJ83-MS7C]; Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1608 (2002).

the source code which is written by programmers using computer languages like python, C++, and Java.[5] The process of transforming the source code to the object code is called compilation.[6] While software companies distribute the object code when licensing programs to end users, they keep the source code secret and unpublished, since it contains valuable information of the software program.[7] To protect software programs, especially the embedded source code, from copying or misappropriation by others, companies consistently rely on IP laws for protection.[8]

Software programs are eligible for different forms of IP protection (e.g., trade secrets, copyright, and patents), as long as they satisfy the corresponding requirements.[9] For example, Article 10 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) considers computer programs as copyrightable literary works whether they are in source or object code.[10] All IP rights, however, have their contours and limits, functioning to balance private monopoly rights and public interest. Patents cannot extend protection to abstract ideas, and copyright only protects expression rather than underlying ideas, while trade secrets law does not prevent proper means, such as reverse engineering and independent development.[11] Recognizing the

---

[5] *See* Daniel Lin, Matthew Sag & Ronald S. Laurie, *Source Code Versus Object Code: Patent Implications for the Open Source Community*, 18 SANTA CLARA COMPUT. & HIGH TECH. L.J. 235, 238-39 (2002); Samuel J. LaRoque, *Reverse Engineering and Trade Secrets in the Post-*Alice *World*, 66 U. KANSAS L. REV. 427, 430 (2017).

[6] *See, e.g.*, Lin et al., *supra* note 5, at 238.

[7] *See* Wallask, *supra* note 4; LaRoque, *supra* note 5, at 431.

[8] *See, e.g.*, LaRoque, *supra* note 5, at 431-35 (discussing how software companies use patent, copyright, and trade secrets to protect their software programs).

[9] *See generally* David Bender, *Trade Secret Protection of Software*, 38 GEO. WASH. L. REV. 909 (1970) (arguing that state trade secrets law provides a feasible and optimal form of protection for software programs); David Bender, *Protection of Computer Programs: The Copyright/Trade Secret Interface*, 47 U. PITT. L. REV. 907 (1986) (discussing whether it is proper for software programs to get benefits of both copyright and trade secrets protection); Michael Risch, *Hidden in Plain Sight*, 31 BERKELEY TECH. L.J. 1635, 1638-52 (2016) (contending that copyright and patent protection leave significant gaps in protecting software programs which can be filled by trade secrets protection); LaRoque, *supra* note 5, at 431-37 (addressing the current limits of patent and copyright protection for software programs and the possibility of protecting them under trade secrets law).

[10] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 10, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) [hereinafter TRIPS Agreement].

[11] *See, e.g.*, Risch, *supra* note 9.

limits inherent in IP laws, many software companies have turned to contract law to supplement protections for their software programs.[12] Anti-reverse engineering clauses are one such example. Reverse engineering of software programs is the process of decompiling, or disassembling, the distributed object code to figure out the source code.[13] Through this process, reverse engineers can "discern or deduce internal design details of the program" to develop a new program for interoperability or to further competitive economic interests.[14] For example, reverse engineering software products requires computer engineers to translate the object code back to the corresponding source code.[15] This is referred to as "disassembly" or "decompilation."[16] To deter attempts at reverse engineering, many technology companies from different countries such as the United States, China, and European Union ("EU") members include anti-reverse engineering clauses in their click-wrap licensing agreements.[17] The goal of such contractual language is to prevent end-users from reverse engineering, decompiling, and disassembling the software object code, regardless

---

[12] *See* David A. Rice, *Public Goods, Private Contract and Public Policy: Federal Preemption of Software License Prohibitions Against Reverse Engineering*, 53 U. PITT. L. REV. 543, 547-48 (1992); Florencia Marotta-Wurgler & Robert Taylor, *Set in Stone? Change and Innovation in Consumer Standard-Form Contracts*, 88 N.Y.U. L. REV. 240, 257 (2013) (using empirical data to show that, during the tested period, the End User License Agreements of software companies have increased contractual restrictions in users' ability to modify the program, create derivative works, and reverse engineer the software); Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1569-70 (2018).

[13] *See* Samuelson & Scotchmer, *supra* note 4, at 1608-09.

[14] *See* Samuelson & Scotchmer, *supra* note 4, at 1608-09.

[15] *See* LaRoque, *supra* note 5, at 438-39.

[16] LaRoque, *supra* note 5, at 438-39.

[17] *See, e.g.*, LaRoque, *supra* note 5, at 441 (offering examples from the United States). For examples from China, see *Agreement on Software License and Service of Tencent Weixin, art. 8.2.1.2*, WECHAT, https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=default&cc=CN [https://perma.cc/8XV9-U3RS] (last visited Jan. 22, 2022); *Douyin End User License Agreement, art. 5.1.2(9)*, ECHINALAW.NET, http://www.echinalaw.net/platform/2021/0720/324.html [https://perma.cc/MK3X-F43N] (last visited Feb. 8, 2022) (Douyin is a Chinese version of Tiktok); *Alipay End User License Agreement and Terms of Service, art. 4.3*, ALIPAY (last updated Dec. 12, 2021), https://render.alipay.com/p/f/fd-iztokkhz/index.html [https://perma.cc/9UJS-PD5D]. For examples from EU members, see Christopher Maierhöfer & Roksana Hosseini, *Contractual Prohibition of Reverse Engineering under the New German Trade Secrets Act – a Practical Guide*, BIRD & BIRD (Jan. 13, 2020), https://www.twobirds.com/en/news/articles/2020/germany/vertraglicher-ausschluss-von-reverse-engineering [https://perma.cc/92QH-ZZY6].

of whether IP laws reach such conduct.[18] Many rising Chinese technology companies have included these terms in their licensing agreements since Chinese law fails to provide clear guidance on the enforceability issue.[19] To access the software, the end users must affirmatively accept these restrictions.[20] Therefore, every user of the software is subject to this contractual restriction, notwithstanding the enforceability issue.

If enforceable, the anti-reverse engineering clauses enable software companies to preclude users from "hijacking" ideas that are not otherwise subject to copyright laws or trade secrets underlying the software. This strengthens the monopoly rights of companies that circumvent the limits of IP rights. Such an extension of IP rights through contract law, however, may disrupt the legislatively designed balance between private rights and the public interest. As Chinese law remains uncertain about whether these terms are enforceable,[21] there is a high risk that this common practice adopted by Chinese software companies may disrupt the private-public balance in China. Accordingly, it is important to explore whether these clauses are enforceable and whether they should be upheld in China. This Article focuses on two main questions: (1) under current Chinese law, *can* anti-reverse engineering clauses be enforced; and (2) if so, *should* these clauses be enforced, considering their impact on the public interest? This Article discusses these questions mainly under the Chinese context. It will compare the positions of China, the United States, and the EU. Through comparative analysis, it strives to provide reform suggestions to clarify the Chinese position on the enforceability issue. This Article is structured as follows: Part II will briefly introduce the current IP protections for software programs and identify the gaps existing in these protections, which software companies use anti-reverse engineering clauses to fill; Part III will then analyze the legal treatment of these restrictive clauses under the Chinese law to demonstrate the uncertainty problem of the Chinese position; Part IV will conduct the comparative analysis by

---

[18] *See* Marotta-Wurgler & Taylor, *supra* note 12, at 257.

[19] *See infra* Part III.

[20] *See, e.g.*, *Terms of Service, Art. 2*, TIKTOK, https://www.tiktok.com/legal/terms-of-service?lang=en [https://perma.cc/U8K8-N8HV] ("By accessing or using our Services, you confirm that you can form a binding contract with TikTok, that you accept these Terms and that you agree to comply with them.").

[21] *See infra* Part IV.

discussing the U.S. and EU positions on this enforceability issue; based on the comparative analysis in Part IV, Part V of this Article will offer suggestions for China's future reform on this issue.

II. IP PROTECTION FOR SOFTWARE PROGRAMS IN CHINA

Software programs may satisfy the requirements of all IP rights, such as copyright, patents, and trade secrets. Companies can choose to protect their programs through copyright, trade secrets, patents, or a combination thereof.[22] This Part will briefly introduce the copyright and trade secrets protection for software programs. It will also discuss the inherent limits set on these IP protections by lawmakers to strike the balance between facilitating economic incentives for innovation and the public's interest in accessing digital information. This Part will also introduce the copyright and trade secrets policies of China. However, it will not discuss patent law because Chinese patent law does not exempt reverse engineering from infringement.[23] Therefore, anti-reverse engineering clauses will not change the rights granted by patent law to software companies, regardless of whether these clauses are enforceable in China. Copyright and trade secrets are more relevant to the topic, as they are normally used together to protect software programs. Moreover, to a certain extent, copyright and trade secrets allow reverse engineering of software programs.

a. Copyright Protection and Reverse Engineering

In China, technology companies can protect their software programs through copyright law. Chinese law on software protection is remarkably similar to U.S. law, which makes it clear

---

[22] *See* Risch, *supra* note 9 (discussing the copyright, patent, and trade secrets protection for software programs); Bender, *Protection of Computer Programs: The Copyright/Trade Secret Interface*, *supra* note 9, at 910 (discussing that many companies use copyright together with trade secret to protect software programs).

[23] *See, e.g.*, FENG XIAOQING, ZHISHI CHANQUAN FA (知识产权法) [INTELLECTUAL PROPERTY LAW] 232-36 (2015) (noting that under Chinese Patent Law, reverse engineering is not one of the exceptions for patent infringement); *cf.* the U.S. position in Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160 (1989) (noting that the right to prohibit reverse engineering was "one of the rights vested in the federal patent holder, but has never been a part of state protection . . . .").

that software programs fall under the ambit of copyright law.[24] The similarity is a result of the U.S.-China Intellectual Property Negotiation (1989), where the Chinese government committed to providing copyright protection for software programs.[25] Under U.S. pressure, the first People's Republic of China (PRC) Copyright Law was enacted in 1990.[26] Article 3(8) explicitly recognized computer software as works that can enjoy copyright rights.[27] This Article remains intact in the version of the PRC Copyright Law amended in 2020.[28] Moreover, the PRC State Council promulgated a specialized regulation about software program protection (hereinafter "Regulation on Computers Software Protection"), adding specific details to the PRC Copyright Law.[29] Combined, software programs are protected mainly by copyright in China.

Copyright law, however, can provide software programs only limited protection. While granting inventors copyright protection can facilitate their incentives to create, over-broad rights may harm the public interest in using the information.[30] Thus, to retain a sound

---

[24] Rice, *supra* note 12, at 573.

[25] *See* U.S. TRADE REPRESENTATIVE, FACT SHEET: "SPECIAL 301" ON INTELLECTUAL PROPERTY 4 (1989), https://ustr.gov/sites/default/files/1989%20Special%20301%20Report.pdf [https://perma.cc/L4PV-TSLM]; *see also* Zhang Jiyu (张吉豫), Ruanjian Fanxiang Gongcheng De Hefaxing Ji Lifa Jianyi (软件反向工程的合法性及立法建议) [The Legitimate Issue of Reverse Engineering Software Programs and Legislative Suggestions], Zhongguo Faxue (中国法学) [4 CHINA LEGAL SCI. 54, 54-55 (2013)].

[26] *See id.*

[27] Zhuzuoquan Fa (著作权法) [Copyright Law] (promulgated by Standing Comm. Nat'l People's Cong., Sept. 7, 1990, effective June 1, 1991), art. 3(8), https://www-pkulaw-com.pennlaw.idm.oclc.org/en_law/59d1a94a76038c6cbdfb.html [https://perma.cc/KK5J-B9EA].

[28] Zhuzuoquan Fa (著作权法) [Copyright Law] (promulgated by Standing Comm. Nat'l People's Cong., Sept. 7, 1990, effective June. 1, 1991, revised by Standing Comm. Nat'l People's Cong., Nov. 11, 2020, effective June 1, 2021), art. 3(8), https://www-pkulaw-com.pennlaw.idm.oclc.org/en_law/a3b3a54bea64f090bdfb.html [https://perma.cc/R65D-FKBH].

[29] Jisuanji Ruanjian Baohu Tiaoli (计算机软件保护条例) [Regulation on Computers Software Protection] (promulgated by State Council, Jan. 4, 1991, effective Oct. 1, 1991, amended by State Council, Jan. 30, 2013, effective Mar. 1, 2013), https://www-pkulaw-com.pennlaw.idm.oclc.org/en_law/41841820b1a1b74abdfb.html [https://perma.cc/PP9Y-N5PB].

[30] *See, e.g.*, Rebecca Tushnet, *Intellectual Property as a Public Interest Mechanism*, *in* THE OXFORD HANDBOOK OF INTELLECTUAL PROPERTY LAW 95-100 (Rochelle Dreyfuss & Justine Pila eds., 2017); Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 248 (1998).

balance between private rights and public interest, the copyright system has certain built-in limitations. First, copyright protection does not extend to ideas underlying software; it protects only the original expressions in the code.[31] Second, copyright excludes functionality, which is reserved for patents and trade secrets,[32] thus implying that copyright law does not protect any functional components of works. This is relevant to software because software is inherently functional.[33] Thus, certain elements in software programs may not receive copyright protection due to their functionality.[34] Meanwhile, copyright law has an important built-in *ex post* limiting mechanism—the fair use doctrine. This doctrine exempts putatively infringing uses from liability if they are deemed fair.[35] This limiting doctrine is relevant to software programs because the Chinese law recognizes certain reverse engineering conduct as fair use.[36] While the current PRC Copyright Law does not permit or prohibit reverse engineering software programs for any other purposes under the copyright law,[37] Article 17 of the

---

[31] *See* WANGQIAN (王迁), ZHISHI CHANQUAN FA JIAOCHENG (知识产权法教程) [INTELLECTUAL PROPERTY LAW TUTORIAL] 45 (6th ed. 2019); *cf.* 17 U.S.C. § 102(b) (2012) (indicating that copyright protection under U.S. law does not "extend to any idea . . . regardless of the form in which it is described, explained, illustrated, or embodied . . . ."); Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1427 (2014) (explaining that in the United States, copyright protection "extends only to the author's original *expression* of a work, not to the underlying ideas, facts, or functional elements of a work"); TRIPS Agreement, *supra* note 9, at art. 9 ("Copyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts . . . .").

[32] *See* WANGQIAN, *supra* note 31, at 55-56; *cf.* 17 U.S.C. § 102(b) (2012) (excluding processes and other functional elements from copyright protection in the United States); Varadarajan, *supra* note 31, at 1427 (indicating exclusion of functional elements from copyright protection in the United States); Risch, *supra* note 9, at 1646 (contrasting copyright with trade secret law in the United States, which can protect functional elements).

[33] *See* Pamela Samuelson, Randall Davis, Mitchell D. Kapor & J.H. Reichman, *Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308, 2320-24 (1994).

[34] *See* WANGQIAN, *supra* note 31, at 55-56; Risch, *supra* note 8, at 1640-41, 1646.

[35] Varadarajan, *supra* note 31, at 1428; Zhuzuoquan Fa (著作权法), *supra* note 28, at art. 24.

[36] *See supra* notes 34-35; *infra* notes 37-41.

[37] The 2020 Amendment of PRC Copyright Law does not include a clause specifically allowing reverse engineering clauses, although the previous published draft of the new Copyright Law included a clause allowing reverse engineering for interoperability. *See* Zhang Jiyu (张吉豫), Ruanjian Jiekou Daima Kezhuzuoxing Yanjiu (软件接口代码可著作权性研究-兼评《著作权法》第三次修改草案"反向工程条款") [Research on the Copyright of Software Interface Code—Comment on the Draft of the Third Revision of the "Copyright Law Reverse Engineering Clause"],

Regulation on Computers Software Protection allows end users to study and research licensed software programs.[38] According to many authors, this can be interpreted as allowing reverse engineering programs for study and research purposes.[39] This clause can also be interpreted as allowing reverse engineering programs for interoperability.[40] In sum, the copyright law in China allows for the reverse engineering of software programs under certain, specified circumstances. These limits are included in the copyright law to justify granting monopoly rights to private parties. To overcome these protection limits and to supplement copyright protection for software programs, many parties look to trade secrets.[41]

b. Trade Secret Protection and Reverse Engineering

The Anti-Unfair Competition Law (AUCL) and its corresponding judicial interpretations constitute the main sources of trade secret protection in China.[42] The trade secrets law in China has

---

Jilin Daxue Shehui Kexue Xuebao (吉林大学社会科学学报) [53 JILIN UNIV. J. SOC. SCI. EDITION 91, 91-92 (2013)]. The new Copyright Law, however, only allows circumventing technological measures to reverse engineer for research purposes. Regulation on Computers Software Protection, s*upra* note 29, at art. 17. Thus, it actually remains uncertain whether reverse engineering software programs for interoperability is allowed in Chinese Copyright Law and for other purposes.

[38] Regulation on Computers Software Protection, s*upra* note 29, at art. 17.

[39] *See e.g.*, Zhang Jiyu, *supra* note 37, at 60; Caowei (曹伟), Ruanjian Fanxiang Gongcheng: Heli Liyong Yu Jieguo Guanzhi (软件反向工程：合理利用与结果管制) [Reverse Engineering Software Programs: Fair Use and Result Regulation], ZHISHI CHANQUAN (知识产权) [4 INTELL. PROP. 23 (2011)].

[40] *See e.g.*, QueZipeng (阙紫鹏), Shehui Chuangxin He Hetong Ziyou De Boyi—Lun Ruanjian Xuke Xieyi Zhong Jinzhi Fanxiang Gongcheng Tiaokuan De Xiaoli (社会创新和合同自由的博弈—论软件许可协议中禁止反向工程条款的效力) [Battles Between Society Innovation and Freedom of Contract—Research on the Enforceability of Anti-Reverse Engineering Clauses in Licensing Agreements], ZHISHI CHANQUAN FA YANJIU(知识产权法研究) [10 INTELL. PROP. RIGHT L. RSCH. 155, 155-56 (2013)]; Zhang Jiyu, *supra* note 25, at 60-61.

[41] *See generally* Bender, *Protection of Computer Programs: The Copyright/Trade Secret Interface*, *supra* note 9, at 910 (introducing a discussion of dual copyright-trade secret protection).

[42] Fan Buzhengdang Jingzheng Fa (反不正当竞争法) [Anti-Unfair Competition Law] (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 2, 1993, effective Dec. 1, 1993; revised by the Standing Comm. Nat'l People's Cong., Nov. 4, 2017; revised by the Standing Comm. Nat'l People's Cong., Apr. 23, 2019), http://lawinfochina.com/display.aspx?id=30315&lib=law [https://perma.cc/8TQH-J7YV]; Zuigao Renmin Fayuan Guanyu Shenli Qinfan

much in common with that in the United States concerning protection requirements and infringement standards, partly because the Chinese trade secrets system has developed under U.S. pressure and influence.[43] Generally, trade secrets have certain advantages over other IP rights. Unlike copyrights and patents, trade secrets can last indefinitely.[44] Trade secrets can cover a wide range of information or products, as long as they satisfy the statutory requirements.[45] Trade secrets can protect unpatentable or uncopyrightable information, so long as this information is kept secret using reasonable measures, is not generally known or readily ascertainable, and can bring independent value for the holders.[46] Software companies customarily keep the source code secret when distributing or licensing software programs, disclosing only the object code.[47] Such limited disclosure of object code satisfies the secrecy requirement of trade secrets.[48] As a result, the eligibility of software programs for trade secrets protection is not in much dispute.[49] Given that software programs are eligible for trade

---

Shangye Mimi Minshi Anjian Shiyong Falv Ruogan Wenti De Guiding, Fashi [2020] Qi Hao (最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定, 法释【2020】7 号) [Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases Involving Infringements upon Trade Secrets No. 7 [2020]] (promulgated by the Judicial Comm. Sup. People's Ct., Sept. 10, 2020, effective Sept. 12, 2020) http://lawinfochina.com/display.aspx?id=34076&lib=law [https://perma.cc/48XJ-LJU3].

43 Although certain procedural rules are very different, such as burden of proof and evidence production, many substantive rules are indeed quite similar. This is because China not only established the trade secrets system due to U.S. pressure but also transplanted many rules from the United States. *See* Yang Chen, *Development of China's Trade Secrets Law in the US' Shadow: Negative Consequences for China and Suggestions*, 17 U. PA. ASIAN L. REV. 138 (2022). For a summary of requirements of trade secrets protection in China, see KONG XIANGJUN, FANBUZHENGDANG JINGZHENG FA XINYUANLI FENLUN (反不正当竞争法新原理分论) [THE NEW PRINCIPLES OF ANTI-UNFAIR COMPETITION LAW: SUBSECTION, at 360-91 (2019)].

44 *See* Varadarajan, *supra* note 31, at 1412.

45 *See* Unif. Trade Secrets Act § 1(4) (Unif. Law Comm'n 1985) [hereinafter UTSA]; Katherine Linton, *The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research*, J. INT'L COM. & ECON. 1, 3 (2016).

46 *See* UTSA § 1(4); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 317-18 (2008).

47 *See* LaRoque, *supra* note 5, at 430-31; Rice, *supra* note 12, at 596.

48 *See* LaRoque, *supra* note 5, at 438.

49 *See, e.g.*, Shangye Mimi Baohu Guiding (Zhengqiu Yijian Gao) (商业秘密保护规定（征求意见稿）) [Regulations on Trade Secrets Protection (Draft for Public Comment)] (promulgated by the State Admin. Mkt. Regul., Sept. 4. 2020), art. 5,

secrets-related protection, the trade secrets law can fill the gaps created by copyright protection; it can protect components of software programs that cannot be copyrighted, such as the underlying ideas and functional elements.[50] This is why many software companies adopt a copyright plus trade secrets approach to protect their programs.[51]

Nevertheless, trade secrets law has one critical limitation—it only protects against misappropriation. In other words, secrets holders cannot rely on trade secrets law to prevent others from obtaining and using trade secrets through proper means.[52] Proper means typically include independent development and reverse engineering.[53] Allowing reverse engineering in trade secrets law is recognized as a significant limiting doctrine, which functions to balance the rights holders' protections and the public interest of

---

http://www.moj.gov.cn/pub/sfbgw/zlk/202009/t20200903_174476.html [https://perma.cc/TL9N-6CL4] [hereinafter 2020 Administration Regulation (Draft)] (recognizing software program source code as trade secrets); Anthony J. Mahajan, *Intellectual Property, Contracts, and Reverse Engineering after* ProCD*: A Proposed Compromise for Computer Software*, 67 FORDHAM L. REV. 3297, 3307-08 (1999); Risch, *supra* note 9, at 1649-50.

[50] *See* Risch, *supra* note 9, at 1646.

[51] *See, e.g.*, Zhao Gang (赵刚), *Shangyemimi Zuixin Sifa Jieshi Dui "Ruanjian" Xiangguang Hangye Shangyemimi Bohu De Yingxiang Ji Jianyi* (*商业秘密最新司法解释对"软件"相关行业商业秘密保护的影响及建议*) [*The Impact of the New Trade Secrets Judicial Interpretation on Software Related Industry and Suggestions*], ZHONG LUN (中伦) (Sept. 30. 2019), http://www.zhonglun.com/Content/2020/09-30/1658438832.html [https://perma.cc/9DBD-XVXT] (discussing the necessity for software companies to use trade secrets to protect software programs, in addition to mere copyright protection); Bender, *Protection of Computer Programs: The Copyright/Trade Secret Interface*, *supra* note 9, at 910; *id.* at 1646-47; LaRoque, *supra* note 5, at 435.

[52] *See* Fan Buzhengdang Jingzheng Fa (反不正当竞争法) [Anti-Unfair Competition Law] (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 2, 1993, effective Dec. 1, 1993; revised by the Standing Comm. Nat'l People's Cong., Nov. 4, 2017; revised by the Standing Comm. Nat'l People's Cong., Apr. 23, 2019), art. 9, http://lawinfochina.com/display.aspx?id=30315&lib=law [https://perma.cc/8TQH-J7YV]; UTSA § 1(1)-(2).

[53] *See* Zuigao Renmin Fayuan Guanyu Shenli Qinfan Shangye Mimi Minshi Anjian Shiyong Falv Ruogan Wenti De Guiding, Fashi [2020] Qi Hao (最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定, 法释【2020】7 号) [Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases Involving Infringements upon Trade Secrets No. 7 [2020]] (promulgated by the Judicial Comm. Sup. People's Ct., Sept. 10, 2020, effective Sept. 12, 2020), Article 14, http://lawinfochina.com/display.aspx?id=34076&lib=law [https://perma.cc/48XJ-LJU3]; UTSA § 1, comment; 18 U.S.C.A. § 1839(6) (B) (West Supp. 2016).

using information for cumulative innovations.[54] In China, the 2007 Judicial Interpretation of AUCL explicitly recognizes reverse engineering as proper means for appropriating trade secrets.[55] In the United States, the Supreme Court even considers allowing reverse engineering a rule designed to weaken trade secrets protection, which is a reason why the trade secrets law is not preempted by federal patent law.[56]

Since trade secrets law cannot prevent reverse engineering conduct, it fails to fill this gap in copyright protection. Software companies, therefore, often resort to contract law by including anti-reverse engineering clauses in licensing agreements.[57] Sample anti-reverse engineering clauses in China state, "You may not . . . [c]onduct *reverse engineering*, *reverse assembly* and *reverse compiling* on the Software, or other attempt to *discover the source code* of the Software."[58] This clause gives software companies broad authority to control the behavior of end-users, far exceeding the rights granted by IP laws. These prohibitory terms try to circumvent the built-in limiting doctrines in IP rights and plausibly disrupt the sound balance intended by these laws. Accordingly, it is valuable to explore whether they are enforceable under current law and, if so, whether they should be enforced in China.

---

[54] *See* Du Kailin (杜开林), "*Fanxiang Gongcheng Jinzhi Tiaokuan" De Xiaoli Yu Shagnye Mimi Baohu* (*反向工程禁止条款"的效力与商业秘密保护*) [*The Effect of Anti-reverse Engineering Clauses and Protections for Trade Secrets*], ZHONGGUO FAMING YU ZHUANLI(中国发明与专利) [5 CHINESE INVENTIONS & PAT. 43, 44 (2005)] (China); Samuelson & Scotchmer, *supra* note 4, at 1583-1584; Stephen J. Davidson, *Reverse Engineering and the Development of Compatible and Competitive Products Under United States Law*, 5 COMPUT. & HIGH TECH. L.J. 399, 401 (1989).

[55] Zuigao Renmin Fayuan Guanyu Shenli Buzhengdang Jingzheng Minshi Anjian Yingyong Falv Ruogan Wenti De Jieshi, Fashi [2007] No. 2 (最高人民法院关于审理不正当竞争民事案件应用法律若干问题的解释, 法释【2007】2 号) [Interpretation of the Supreme People's Court on Some Issues Concerning the Application of Law in the Trial of Civil Cases Involving Unfair Competition, Judicial Interpretation [2007] No. 2] (promulgated by the Judicial Comm. Sup. People's Ct., Jan. 12, 2007, effective Feb. 1, 2007), art. 12, https://www.pkulaw.com/en_law/e7b897dddc93e2fabdfb.html [https://perma.cc/SXW4-7ZNV].

[56] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 489-90 (1974).

[57] *See supra* notes 12-19 and accompanying text.

[58] *See* WECHAT, *supra* note 17.

III. DESCRIPTIVE ANALYSIS: CURRENT LEGAL STATUS IN CHINA

While software companies in China frequently include anti-reverse engineering in licensing agreements,[59] the position of Chinese law on whether these terms are enforceable is less clear. Cases directly dealing with the enforceability issue in China are scant. One early case, however, partly touched this issue and can provide some relevant insight.[60] This case concerned a clause in the licensing agreement which prohibited any reverse engineering, decompiling, or disassembling of software programs, unless the applicable law allowed the restricted behaviors.[61] The defendant argued that since Chinese copyright law did not explicitly prohibit reverse engineering and that doing so was his basic right, this contract term unduly increased his liability and foreclosed his basic right.[62] Hence, he argued that such a term should be void.[63] The Beijing First Intermediate Court, however, rejected his argument and upheld this term.[64] It reasoned that, because the Chinese law did not specifically prohibit the use of anti-reverse engineering terms, the argument that such a term violated basic rights was not persuasive.[65]

The reasoning of this court can thus provide certain insights about the treatment of these prohibitory terms in China. The result in this case seems to support the proposition that these terms are enforceable in China. However, it is not that simple. The decision does not set a precedent about the enforceability of anti-reverse engineering clauses because it was not the main issue in this case. The court's decision is based on other standard terms included in licensing agreements.[66] There is only one sentence mentioning the

---

59 *See supra* note 17 and accompanying text.

60 *See* WeiruanGongsi Yu Guoli Deng Jisuanji Ruanjian Zhuzuoquan Xuke Shiyong Hetong JiufenYian (微软公司与郭力等计算机著作权许可使用合同纠纷一案) [Microsoft Co. v. Guo Li, A Dispute Over Computer Copyright Licensing Contract Dispute] (Beijing High People's Ct. June 20, 2013) (China), http://bjgy.chinacourt.gov.cn/paper/detail/2013/07/id/1096065.shtml [https://perma.cc/CS4P-MM5B].

61 *Id.*

62 *Id.*

63 *Id.*

64 *Id.*

65 *Id.*

66 *Id.*

enforceability issue without any detailed reasonings.[67] Also, it may be argued that the enactment of the 2020 amendment of PRC Copyright Law changed this aspect of the ruling as it now allows circumventing technological measures to reverse engineer software.[68] Therefore, this case has limited precedential value for courts. Based just on this early case, we cannot conclude that the Chinese law allows enforcement of these prohibition terms.

Although few cases in China touch on the enforceability issue in practice, academia has provided valuable arguments and insights about whether these terms are enforceable based on Chinese policy considerations. Most scholars argue that these prohibition terms should be invalid based on the invalidity doctrine in contract law.[69] The doctrine of contract invalidity in China is based on Article 52 of the PRC Contract Law, which has been codified into Article 153 of the new PRC Civil Code.[70] According to Article 52 of the PRC Contract Law, any contract terms which conflict with the public order and good customs (the first prong), or with mandatory provisions in laws and regulations (the second prong), are invalid.[71] However, differences exist among these scholars regarding how the doctrine applies in invalidating anti-reverse engineering terms. Some argue for using the public order and good customs prong (the first prong) to invalidate these terms.[72] They contend that, because

---

[67] *Id.*

[68] Zhuzuoquan Fa (著作权法) [Copyright Law] (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 7, 1990, rev'd Nov. 11, 2020, effective June. 1, 2021), art. 50 https://www-pkulaw-com.pennlaw.idm.oclc.org/en_law/59d1a94a76038c6cbdfb.html [https://perma.cc/KK5J-B9EA].

[69] *See e.g.*, Zhang Jiyu, *supra* note 25, at 61; Caowei, *supra* note 39, at 24-25; Chen Shan (陈珊), Jinzhi Ruanjian Fanxiang Gongcheng Tiaokuan De Xiaoli Yanjiu—Yi Fayi Baohu Wei Shijiao (禁止软件反向工程条款的效力研究——以法益保护视角) [Research on the Enforceability of Reverse Engineering Prohibition Terms—From the Perspective of Protecting Legal Interests], Kaifeng Jiaoyu Xueyuan Xuebao (开封教育学院学报) [38 J. KAIFENG INST. EDUC. 242 (2018)]; QueZipeng, *supra* note 40, at 164-66.

[70] Hetong Fa (合同法) [Contract Law] (promulgated by the Standing Comm. Nat'l People's Cong., Mar. 15, 1999, effective Oct. 1, 1999, invalidated by the Civil Code, Jan. 1, 2021), art. 52, http://lawinfochina.com/display.aspx?id=6145&lib=law [https://perma.cc/DG9S-8X77]; codified into Minfa Dian (民法典) [Civil Code] (promulgated by the Standing Comm. Nat'l People's Cong., May 28, 2020, effective Jan. 1, 2021), art. 153, http://lawinfochina.com/display.aspx?id=32806&lib=law [https://perma.cc/SX7N-4VCP].

[71] *Id.*

[72] *See, e.g.*, Zhang Jiyu, *supra* note 25, at 61; Chen Shan, *supra* note 69, at 242.

prohibitory terms protect those parts of programs that are not copyrightable, these terms are at odds with the interest of the public.[73] Such prohibitions amount to a patent-like protection without passing high protection thresholds set by patent law and thus erode the private-public balance set within.[74] Thus, based on the negative impact of these terms on public interest, these authors argue that these terms are invalid because they harm the public order and good customs.[75] Some, nevertheless, argue for using the prong of mandatory provisions of laws and regulations (the second prong) to strike down these terms.[76] They consider Article 17 of the Regulation on Computers Software Protection as a mandatory provision in the regulation.[77] Since the contract terms are against the mandatory provision of Article 17, they should be invalidated, according to the doctrine of contract invalidity.[78] In addition, others who use this mandatory provision prong consider the provision allowing reverse engineering in Chinese trade secrets law (Article 12 of 2007 Judicial Interpretation of AUCL) as mandatory provisions in law.[79] According to their opinion, these prohibitory terms are invalid because they directly conflict with 2007 Judicial Interpretation of AUCL's reverse engineering provision.[80] In this regard, although all these authors support striking down these terms using the same doctrine, disputes still exist as to how exactly to invalidate them.

These disputes result from the inherent uncertainty and vagueness of the contract invalidity doctrine in contract law, which itself is much debated.[81] As a well-known Chinese contract law scholar notes, the notion of public order and good customs is inherently uncertain, with no clear definitions.[82] It largely depends on the judge in the disputed cases to interpret this notion and take the policy considerations into account. How the judge will interpret this notion in cases concerning anti-reverse engineering clauses is

---

73 *See supra* note 72.

74 *See, e.g.*, Caowei, *supra* note 39, at 25.

75 Caowei, *supra* note 39, at 25.

76 *See, e.g.*, QueZipeng, *supra* note 40, at 164-66.

77 QueZipeng, *supra* note 40, at 164-66.

78 QueZipeng, *supra* note 40, at 164-66.

79 *See, e.g.*, Du Kailin *supra* note 54, at 44.

80 Du Kailin *supra* note 54, at 44.

81 *See, e.g.*, HAN SHIYUAN (韩世远), HETONGFA ZONGLUN (合同法总论) [THE LAW OF CONTRACTS] 228-29 (4th ed., 2018).

82 *Id.*

unpredictable. Although these prohibitory clauses may disrupt the patent and copyright law policy, they incentivize innovators to create, which is also an important policy of IP laws. Thus, it remains unclear as to how the courts may balance these equally important policy considerations underlying IP laws in deciding whether these terms harm public order and good customs. Similar problems exist in the mandatory law and regulation prong. The scope of mandatory provisions of laws and regulations is uncertain and remains a complicated issue. Article 153 of new PRC Civil Code provides that if the mandatory provision in the laws or regulations does not render contracts invalid, then Article 153 does not apply.[83] This leaves unsettled the question of which mandatory provision Article 153 applies to. Many scholars have struggled to define the mandatory provisions in laws and regulations under Article 153 and provided quite complex standards in drawing the line.[84] With such a vague and unclear definition of mandatory provisions, it is questionable whether courts may consider Article 17 of the Regulation on Computers Software Protection or the 2007 Judicial Interpretation of AUCL's reverse engineering provision as mandatory provisions as per Article 153 of the Civil Code. That being said, using such a vague and largely debatable doctrine reduces the persuasiveness of these authors' arguments. It remains unknown, in using this doctrine, how the court in the future may consider the public policy issues concerned or whether the court will consider the relevant Articles as mandatory provisions as per Article 153 of the Civil Code. Although the policy considerations underlying these scholars' arguments are reasonable, contract law's invalidity doctrine is too vague to solve the enforceability issue, as it excessively relies on the unpredictable interpretations of courts.

The position of Chinese law on the enforceability of anti-reverse engineering clauses is remarkably unclear. Though one case discussed the issue, it was decided on entirely separate grounds.[85] Moreover, the case has become outdated following the more recent

---

[83] Minfa Dian (民法典) [Civil Code] (promulgated by the Standing Comm. Nat'l People's Cong., May 28, 2020, effective Jan. 1, 2021), art. 153, http://lawinfochina.com/display.aspx?id=32806&lib=law [https://perma.cc/SX7N-4VCP].

[84] *See, e.g.*, Yang Daixiong (杨代雄), <*Minfadian*> *Di 153 Tiao Diyi Kuan Pingzhu* (《民法典》第 153 条第 1 款评注) [Comments on the First Provision of the Article 153 of the Civil Code], Fazhi Yanjiu (法治研究) [5 RSCH. ON RULE L. 129, 129-32 (2020)] (classifying mandatory provisions in law and regulation into four types and discussing whether each type is within the scope of Article 153).

[85] *See supra* notes 60-68.

legal developments in China.[86] Scholars have argued that these terms are invalid because of the invalidity doctrine, but the inherent vagueness and controversy surrounding this doctrine make it uncertain how courts may apply it to invalidate these terms. Thus, uncertainty persists in China about whether anti-reverse engineering terms are enforceable. This uncertainty should be resolved as soon as possible because "the public and private right owners deserve to know in advance the precise level of proprietary protection they can expect so that they may conduct themselves accordingly."[87] To deal with the uncertainty, other countries' positions can provide valuable insights for potential reform suggestions for China.

IV. COMPARATIVE ANALYSIS: CURRENT LEGAL STATUS IN THE UNITED STATES AND EU

a. A Threshold Question: Why the United States and EU?

An initial question that we should address before starting the comparative analysis is why we should be comparing China with the United States and the EU. One reason is that U.S. law consistently affects the development of Chinese IP laws due to the long-existing U.S.-China trade relations.[88] Indeed, not only was the first PRC Copyright Law promulgated due to a U.S.-China trade deal,[89] but also the Chinese trade secrets law develops in the shadow of U.S. pressure and influence.[90] With the inherent influence of U.S. law on the Chinese IP laws, it is natural, when discussing reform suggestions for IP issues in China, to see what the U.S. position is and whether China can follow suit. Moreover, compared with the uncertain Chinese position, the U.S. position is much clearer, and the U.S. courts have already, in several cases, offered valuable policy

---

86 *See supra* notes 60-68.

87 Mahajan, *supra* note 49, at 3325.

88 *See, e.g.*, Peter K. Yu, *A Half-Century of Scholarship on the Chinese Intellectual Property System*, 67 AM. U. L. REV. 1045, 1065-70 (2018) (discussing U.S. influence on the development of Chinese IP systems).

89 *See supra* notes 25-28 and accompanying text.

90 *See generally* Chen, *supra* note 43 (discussing how China's trade secrets law developed under U.S. influence and pressure).

considerations concerning this enforceability issue.[91] Thus, there are certainly valuable lessons for China to learn from U.S. law. Furthermore, the EU has even more straightforward rules than the United States as it has specific statutory provisions and cases focusing on this issue.[92] In this sense, exploring the United States and EU positions can assist us in providing more reliable reform suggestions for China.

b. Anti-reverse Engineering Clauses in the United States

Most U.S. courts currently address the enforceability of anti-reverse engineering clauses through the preemption doctrine, which holds that federal law prevails over any conflicting state law or regulation[93]; they often ask, for example, whether federal copyright law preempts the relevant state contract law. This is understandable because anti-reverse engineering clauses prevent end users from studying and using those components of software programs that cannot be copyrighted.[94] In this sense, state contract law seems to create copyright-like exclusive rights over those elements that cannot be copyrighted otherwise. In other words, the state contract law, in essence, extends the federal copyright protection to uncopyrightable elements. Thus, it is arguable that the federal copyright law may preempt the state contract law in enforcing anti-reverse engineering clauses. To elaborate on this point, the first section of this Part will discuss the enforceability issue under the federal copyright law preemption doctrine. Apart from this, since trade secrets law may also provide software companies a stand-alone cause of action, this Part will discuss the enforceability issue under the federal trade secrets and federal patent laws as well.

---

91 *See infra* Part V.B.

92 *See infra* Part V.C.

93 NOAM SHEMTOV, BEYOND THE CODE: PROTECTION OF NON-TEXTUAL FEATURES OF SOFTWARE 51 (2017).

94 *See* Jisuanji Ruanjian Baohu Tiaoli (计算机软件保护条例) [Regulation on Computers Software Protection] (promulgated by State Council, Jan. 4, 1991, effective Oct. 1, 1991, amended by State Council, Jan. 30, 2013, effective Mar. 1, 2013), art. 17 and accompanying text, https://www-pkulaw-com.pennlaw.idm.oclc.org/en_law/41841820b1a1b74abdfb.html.

i. Enforceability Under Federal Copyright Law

One notable case which turned down these anti-reverse engineering clauses is *Vault Corp. v. Quaid Software Ltd*. *Vault* was concerned with a state statute that explicitly allowed software companies to include licensing terms to restrict, or even prohibit altogether, reverse-engineering the object code.[95] The Fifth Circuit ruled that this statutory provision "clearly 'touches upon an area' of federal copyright law," making it preempted.[96] As a result, the court invalidated the anti-reverse engineering terms in Vault's licensing agreement.[97] However, the Fifth Circuit did not provide detailed reasoning for the preemption issue, and this case had special facts that a state statute was concerned with. This has made *Vault* easily distinguishable, thus enabling future courts to allow the enforcement of limiting provisions.[98] Indeed, many courts after *Vault* chose to uphold the terms by distinguishing with *Vault*.[99]

The Federal Circuit in *Bowers v. Baystate Techs., Inc.*, applying the law of the First Circuit, upheld the prohibition on reverse engineering in the license agreements.[100] According to the law of the First Circuit, preemption by federal copyright law did not apply if "a state cause of action requires an *extra element*, beyond mere copying, preparation of derivative works, performance, distribution or display."[101] The law of the First Circuit allowed the enforcement of state contractual rights, holding that the Copyright Act did not preempt contract claims.[102] This is because contracts "generally affect only their parties" and do not create "exclusive rights," in contrast to a copyright which is an exclusive right against the world.[103] Since the state enforcement of contractual terms prohibiting reverse engineering did not create an "exclusive right" against the world, this court allowed the enforcement of these

---

95 Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 268-69 (5th Cir. 1988).

96 *Id.* at 270.

97 *Id.*

98 *See e.g.*, Bowers v. Baystate Techs., Inc., 320 F.3d 1317 (Fed. Cir. 2003); Davidson & Assocs. v. Jung, 422 F.3d 630 (8th Cir. 2005).

99 *See supra* note 98.

100 *Bowers*, 320 F.3d at 1322-23.

101 *Id.* at 1324 (emphasis added).

102 *Id.* at 1325.

103 *Id.*

provisions.[104] The Federal Circuit distinguished this case from *Vault*, noting that *Vault* was concerned with a state statute, while this case was strictly solely about private contractual agreements.[105] Since the prohibitory terms were upheld, this court supported the claim of breach of contract.[106]

Although the dissenting opinion in *Bowers* objected to the ruling and supported *Vault* on this issue,[107] other circuits showed a propensity to follow *Bowers* rather than *Vault*. For example, the Eighth Circuit, in *Davidson & Assocs. v. Jung*, endorsed *Bowers* and allowed the enforcement of anti-reverse engineering clauses.[108] The court distinguished the case from *Vault* for the same reason—*Vault* was concerned with a state statute, while this case was about private restrictions on reverse engineering in licensing agreements.[109] The *Davidson* court considered this case more similar to *Bowers*, where end-users expressly relinquished the rights to reverse engineering in license terms.[110] *Davidson* thus endorsed the reasoning in *Bowers* and enforced the contractual limitations.[111]

Although *Vault* remains good law in the Fifth Circuit, it is frequently distinguished by other courts, as best illustrated by the decisions of the Federal and Eighth Circuits.[112] Prior relevant case law reveals a trend of courts enforcing anti-reverse engineering terms, at least under copyright law. Indeed, empirical evidence has shown that the courts' welcoming position has empowered software companies to use anti-reverse engineering clauses in their terms of services more frequently.[113] The analysis, however, does not end here. Although, according to many courts, anti-reverse engineering clauses do not touch on the exclusive area of federal copyright law, they may, in certain circumstances, be directly in conflict with federal trade secrets and patent laws. The analysis must therefore consider the possibility of federal trade secrets or patent preemption.

---

104 *Id.*

105 *Id.*

106 *Id.* at 1326.

107 *Id.* at 1335 (Dyk, J., dissenting).

108 422 F.3d 630 (8th Cir. 2005).

109 *Id.* at 639.

110 *Id.*

111 *Id.*

112 *See* Bowers v. Baystate Techs., Inc., 320 F.3d 1317 (Fed. Cir. 2003); Davidson & Assocs. v. Jung, 422 F.3d 630 (8th Cir. 2005).

113 Marotta-Wurgler & Taylor, *supra* note 12, at 257.

ii. Enforceability Under Federal Trade Secrets Law

While no case currently touches on this issue, it remains possible that such anti-reverse engineering clauses may be preempted by federal trade secrets law, specifically the Defend Trade Secrets Act (DTSA) of 2016. The DTSA expressly allows the reverse engineering of trade secrets by excluding it from improper means.[114] In light of this language, it is questionable whether a contractual prohibition of reverse engineering can withstand the preemption test of the DTSA. The DTSA has a preemption exception, which states that it does not "preempt or displace any other remedies, whether civil or criminal, provided by [U.S.] Federal, State, commonwealth, possession, or territory law *for the misappropriation of a trade secret*."[115] Arguably, this preemption exception applies only to state trade secrets law rather than others, such as state enforcement of contractual terms.[116] Accordingly, it seems that the DTSA is likely to preempt the enforcement of contractual bans on reverse engineering, since state contract law is not explicitly included in the preemption exception.

Nevertheless, there is an argument that, even if this preemption exception does include state contract law, courts may still enforce anti-reverse engineering terms. This is because courts may still follow the previous reasoning for preemption (see, for example, *Bowers*), which considers trade secrets rights as rights against the world, like copyright.[117] Following this logic, since contractual rights are mere rights between parties rather than rights against the world, contractual bans on reverse engineering do not fall within the scope of the DTSA, which is concerned with rights against the world.[118] Therefore, such contractual bans would not be preempted by the DTSA. This argument is becoming increasingly convincing, since trade secrets are often considered a type of IP right, on the same footing as copyright, patents, and trademarks.[119] With

---

114 Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 2(b)(6)(B), 130 Stat. 376, 381.

115 18 U.S.C.A. § 1838 (West Supp. 2016) (emphasis added).

116 *See* LaRoque, *supra* note 5, at 449-50.

117 *Id.* at 450. The *Bowers* court believed that the first circuit followed the reasoning of *ProCD* and held that contracts do not create exclusive rights so that the Copyright Act does not preempt contract claims. *Bowers*, 320 F.3d at 1324-25.

118 *See* LaRoque, *supra* note 5, at 450.

119 *See e.g.*, Lemley, *supra* note 46, at 329-41; Varadarajan, *supra* note 31, at 1418-20; Eric Goldman, *The Defend Trade Secrets Act Isn't an 'Intellectual Property' Law*, 33 SANTA CLARA HIGH TECH. L.J. 541 (2017) (arguing that DTSA should have explicitly

increasing support for treating trade secrets as IP rights, courts are more likely to adopt the view that trade secrets are exclusive rights, like copyright, to validate contractual bans. Thus, while one can reasonably argue against enforcement of these terms under DTSA, such an argument may not ultimately be that strong.

iii. Enforceability Under Federal Patent Law

Although the result of a DTSA preemption analysis does not figure to affect the copyright preemption result, patent preemption analysis may make the enforceability of these prohibitory clauses highly questionable. Patent preemption is the result of the controversial relationship between trade secrets and patents. In *Kewanee Oil Co. v. Bicron Corp.*, the Supreme Court held that state trade secrets law was not preempted by the Federal Patent Law, partly because trade secrets did not constitute an equivalent to patents, since trade secrets offered much weaker protections.[120] Reverse engineering, according to the court's opinion, functions exactly like the limiting doctrine weakening the trade secrets protection.[121] In other words, it is fair to say that allowing reverse engineering of trade secrets was a critical reason why the Supreme Court upheld the trade secrets law in *Kewanee*.[122] Allowing the enforcement of anti-reverse engineering clauses to supplement trade secrets protections may make state law protections more equivalent to patents. Therefore, it seems to be directly against the ruling in *Kewanee* if reverse engineering can be effectively prohibited by contractual terms. In other words, contractual bans on reverse engineering are likely to be unenforceable following the *Kewanee* line of thought.

Although no court after *Kewanee* has specifically discussed the patent preemption issue of prohibitory terms on reverse engineering, at least some courts have shown an inclination to invalidate such terms based on patent preemption. In *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, citing *Kewanee,* the court ruled that

---

recognized trade secrets as a type of IP); *cf.* Bone, *supra* note 30, at 248; Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803 (2014) (arguing against the view that trade secrets should be treated as IP rights).

120 416 U.S. 470, 489-90 (1974).

121 *See id.* at 489-92.

122 Rice, *supra* note 12, at 623.

the relevant state law, which prohibited reverse engineering a product in the public domain, was preempted by federal patent law.[123] The court reasoned that the right to prohibit reverse engineering was "one of the rights vested in the federal patent holder, but has never been a part of state protection . . . ."[124] Notwithstanding the fact that *Bonito* does not directly touch the enforceability issue of contractual terms, its reasoning arguably shows that bans on reverse engineering, regardless of their form, are governed exclusively by federal patent law, which state laws should not contravene.

While no case has directly ruled on the enforceability of contractual prohibitions on reverse engineering under federal patent law, influential cases such as *Kewanee* and *Bonito* offer ample room for invalidating these contractual bans based on patent preemption. However, the subject matter covered in *Kewanee* and *Bonito* is not directly related to the software industry. *Kewanee* and *Bonito* addressed the enforceability issue in the traditional manufacturing industry,[125] which is very different from the newly developed software industry. The software industry has many special features (for example, it is more incremental and cumulative than traditional manufacturing industries) that we should take into consideration in the legal analysis.[126] It is not appropriate to make the direct inference that the rules and reasoning in cases related to other traditional industries can wholly apply to a quite different and relatively new industry.[127]

The question of the extent to which the law should regulate reverse engineering or allow private ordering on reverse engineering may better be answered in each industry's context.[128] Reverse engineering is justified to the extent that a sufficient lead time is preserved for rights holders, while reserving ample room for later entrants to author cumulative innovations.[129] For example, it

---

123 Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160 (1989).

124 *Id*.

125 *See Kewanee*, 416 U.S. at 470; *Bonito Boats*, 489 U.S. at 144-45.

126 Samuelson et al., *supra* note 33, 2330-32; LaRoque, *supra* note 5, at 439-40.

127 For an argument that rules concerning reverse engineering should differentiate from industries, see generally Samuelson & Scotchmer, *supra* note 4.

128 *See generally* Samuelson & Scotchmer, *supra* note 4 (discussing the economic soundness of regulations on reverse engineering in each industry and promoting for different treatment of reverse engineering in different industries).

129 *See* Rice, *supra* note 12, 570-71; Samuelson & Scotchmer, *supra* note 4, at 1649-50.

seems more suitable to allow private prohibitions on reverse engineering if competitors may easily reverse engineer, thus providing sufficient lead time for rights holders. However, these prohibitions should not provide rights holders with indefinite control over information embedded in their products, fully precluding the public's use and benefit. At what point this balance should lie differs across industries (for example, traditional manufacturing industries, computer software industry).

The software industry has special features we must take into consideration. First, the software industry is incremental and cumulative, such that programmers not only contribute to, but also benefit from, the innovation process.[130] Since software products "almost invariably contain admixtures of old and new elements," this weighs in favor of finding that allowing a total contractual ban on reverse engineering would not be a sound practice in the software industry.[131] Another notable feature of the software industry is that technological development has gradually made reverse engineering software programs increasingly easier and cheaper, leaving rights holders much less lead time.[132] A straightforward invalidation of anti-reverse engineering clauses may disrupt right holders' incentives to innovate to an unjustifiable degree.

Applied to the patent preemption point and considering the unique context of the software industry, courts may apply *Kewanee* or *Bonito* in modified ways to account for specific industry needs. First, the enforcement of a total contractual ban on reverse engineering for any purpose is likely to be held as preempted by federal patent law. One reason is that such a ban would effectively create an absolute and indefinite right for software program creators. This would upset the balance between granting monopoly rights and upholding the public's needs for information. Moreover, it would directly conflict with the ruling in *Bonito*.[133] Another reason is that such a ban may destroy the industry's demands for cumulative innovations and thus result in overly negative policy implications. Therefore, a total ban on reverse engineering in the software industry cannot survive the preemption test under *Kewanee* or *Bonito Boats*, just as in the traditional manufacturing industry.

---

130 Samuelson et al., *supra* note 33, at 2330-32.

131 Samuelson et al., *supra* note 33, at 2332.

132 *See* LaRoque, *supra* note 5, at 439-40.

133 Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 157-58 (1989).

Nevertheless, given that current software reverse engineering technology has eroded much of the lead time enjoyed by the program creators, courts may aim to partly distinguish cases in the software industry with *Kewanee* or *Bonito,* which is in the manufacturing industry. Courts may show more sympathy for anti-reverse engineering clauses in the software industry, so long as they do not go too far. For example, a limited contractual ban on reverse engineering programs may be more likely to pass the patent preemption test than a total ban. One example of a limited ban would be a contractual limitation on reverse engineering for producing directly competing programs.[134] This contract term does not preclude reverse engineering for other purposes, such as interoperability or research and study.[135] Such a limited ban is arguably more likely to pass the patent preemption test of *Kewanee* or *Bonito* because it preserves a sufficient lead time for software companies by deterring reverse engineering for direct competition while reserving enough room for the public to reverse engineer for other purposes such as cumulative innovations.[136] This limited ban does not disrupt the patent law's balance and the software industry's cumulative nature. Therefore, while a total contractual ban is likely to be invalid, such a limited ban may be plausibly upheld.

iv. Summary and Insights

Although the position of U.S. law on the enforceability issue of anti-reverse engineering clauses is complex and often ambiguous, some concrete observations can be made. Cases under federal copyright preemption show that these prohibitory terms are not preempted by federal copyright law. Federal trade secrets preemption does not seem to change the enforceability of their limits either, as the argument for DTSA preemption is quite weak. Federal patent law preemption, however, may render anti-reverse engineering clauses unenforceable, as they may unduly disrupt the federal patent law policy in balancing monopoly rights with public benefit of access to the information (i.e., cumulative innovations).

---

134 LaRoque, *supra* note 5, at 453.

135 LaRoque, *supra* note 5, at 453.

136 LaRoque, *supra* note 5, at 453-55.

Nevertheless, considering the unique landscape of the software industry, courts may not adopt a one-size-fits-all approach in dealing with the enforceability issue. Plausible predictions can be made based on previous rulings on patent preemption cases in traditional manufacturing industry. For example, in recognizing the special needs and situations of the software industry, courts are more likely to invalidate the total contractual bans on reverse engineering, while enforcing the limited bans.

The descriptive analyses and predictions of the enforceability of anti-reverse engineering clauses under U.S. law can inform an effective normative analysis of reform suggestions for China, as the enforceability issue in China shares many common policy implications and choices with that in the United States. Before discussing normative suggestions and how exactly this descriptive analysis in the United States helps the normative analysis, the following section will then discuss the EU position on this enforceability issue and explore what additional insights the EU law can bring to the normative analysis.

c. Anti-reverse Engineering Clauses in the EU

The EU law recognizes two forms of reverse engineering—"black box" reverse engineering and decompilation.[137] "Black box" reverse engineering means running and loading a software program to study and research the program so as to uncover the ideas and principles underlying the program.[138] Article 5(3) of the EU Computer Programs Directive clearly exempts this type of reverse engineering from copyright infringement.[139] Article 8 of this Directive clearly prohibits any contractual provisions to the contrary.[140] Thus, under the EU law, contractual limitations on reverse engineering for research and study purposes are not enforceable. Moreover, the EU law exempts any decompilation acts attempting to transfer the object code of the program to the source code for interoperability purposes.[141] In other words, end-users have the rights to decompile a software program to obtain the

---

137 *See* SHEMTOV, *supra* note 93, at 72-73.

138 *See* SHEMTOV, *supra* note 93, at 71.

139 Council Directive 2009/24, art. 5(3), 2009 O.J. (L 111) 16, 19 (EC).

140 Council Directive 2009/24, art. 8, 2009 O.J. (L 111) 16, 19 (EC).

141 Council Directive 2009/24, art. 6, 2009 O.J. (L 111) 16, 19 (EC).

underlying interface information,[142] which allows users to develop compatible applications. Again, this right to decompile for achieving interoperability cannot be waived contractually.[143] In summary, the EU law explicitly disallows any prohibitive contract terms on reverse engineering for research and study purposes or for achieving interoperability. Reverse engineering for other purposes may amount to copyright infringement, and software companies are certainly free to include relevant limiting terms in licensing agreements to add the protection.[144]

The policy rationales backing these straightforward rules are evident. Firstly, they aim to protect the public interest to view, use, and study the ideas of a program while preserving enough rights for program owners.[145] Secondly, they promote interoperability to deter platform monopolies that do not benefit consumer welfare.[146] This is because reverse engineering for interoperability is normally intended to obtain the application programming interfaces (APIs) of platforms, so as to develop compatible applications.[147] Without reverse engineering, application developers have to accept the strict and less-friendly terms provided by platforms, such as agreeing not to run applications on rival platforms, which gives platform holders excessive power in the market.[148] This arrangement unduly dampens the incentives of developers to create new applications and benefits platform holders. Although allowing reverse engineering for interoperability may slightly affect the monopoly rights enjoyed by rights holders and, in turn, negatively impact the incentives to develop platforms, it increases incentives to develop applications and improves competition in the platform market. On balance, public welfare benefits more from allowing reverse engineering for interoperability because consumers can enjoy more applications in different platforms and the system price of platforms may be lower in the long run due to the enhanced competition.[149]

Reform suggestions for the Chinese law can shed much light on these straightforward rules and their underlying policy

---

142 *See* SHEMTOV, *supra* note 93, at 80.

143 Council Directive 2009/24, art. 8, 2009 O.J. (L 111) 16, 19 (EC).

144 *See* SHEMTOV, *supra* note 93, at 72-73 (noting that it is only decompilation to achieve interoperability that might be excused).

145 *See* SHEMTOV, *supra* note 93, at 83-84.

146 *See* SHEMTOV, *supra* note 93, at 79-80.

147 *See* Samuelson & Scotchmer, *supra* note 4, at 1615-16.

148 *See* Samuelson & Scotchmer, *supra* note 4, at 1617-18.

149 *See* Samuelson & Scotchmer, *supra* note 4, at 1621.

considerations. The next Part, thus, will further the comparative analysis by providing reform proposals for China based on the insights from the U.S. and EU positions.

V. LEGAL REFORM SUGGESTIONS FOR CHINA: AN INTERMEDIATE APPROACH

Before normatively discussing suggestions concerning Chinese legal reform on anti-reverse engineering clauses, a threshold question must be addressed: *which forum should be relied upon to deal with the uncertainty of this legal issue?* This Article considers that, to eliminate the uncertainty, courts are not an ideal venue. This is because different courts may adopt inconsistent or contradictory approaches, which may actually add to the uncertainty. The situation is even more serious in China, which is not a common law country. This means that Chinese courts should normally base their decisions on statutes, rather than previous case laws.[150] The most plausible doctrine which Chinese courts may use is the contract law validity doctrine. However, it is inherently vague and undetermined.[151] Therefore, it is more appropriate for China to follow the EU to adopt explicit provisions in either statutes or judicial interpretations rather than relying on courts in individual cases.

---

[150] The situations may have slightly changed after the SPC's issuance of the "Guiding Opinions of the Supreme People's Court on Unifying the Application of Laws to Strengthen the Retrieval of Similar Cases (for Trial Implementation)", which requires courts in certain cases (normally complex cases) to do a preemptive search for similar cases from higher courts (or cases these courts themselves decide) and follow suit. *See* Zuigao Renmin Fayuan Guanyu Tongyi Falv Shiyong Jiaqiang Leian Jiansuo De Zhidao Yijian (Shixing) (最高人民法院关于统一法律适用加强类案检索的指导意见(试行)) [Guiding Opinions of the Supreme People's Court on Unifying the Application of Laws to Strengthen the Retrieval of Similar Cases (for Trial Implementation)] (promulgated by the Judicial Comm. Sup. People's Ct., July 1, 2020, effective Jul. 31, 2020), https://www.pkulaw.com/en_law/0749b01d6f2da00dbdfb.html [https://perma.cc/J37S-4DRR]. However, statutes still remain the main source for each case and this judicial guiding opinion only applies to a limited scope of cases.

[151] *See supra* Part III.

a. The One-Size-Fits-All Approach is Not Appropriate for China

A possible approach to deal with anti-reverse engineering clauses is adopting the one-size-fits-all treatment for these clauses: a straightforward provision prohibiting the use of anti-reverse engineering clauses or allowing their use, regardless of what purpose the reverse engineering is for. Nevertheless, this Article argues that the one-size-fits-all approach does not suit the Chinese context. The first choice may be enforcing these terms, regardless of what type of reverse engineering behaviors are prohibited. If we look solely at copyright preemption cases, U.S. law supports this choice.[152] As previous U.S. copyright preemption cases indicate, state contract law should be respected. By respecting state contract law, one of the embedded purposes of U.S. courts is to respect the freedom of contract.[153] Considering the importance of the freedom of contract, it seems sound for China to allow parties to freely decide what rights are limited and what are granted. Freedom of contract, however, should not be boundless. When there are sufficient reasons, such as important policy considerations like the public interest, it is justifiable that the law partly restricts contract freedom. Further, in the software licensing context, it is doubtful whether the signing of licensing agreements is truly free. Standard licensing terms or, more specifically, "click-wrap" terms, are always used in the software licensing scenario, which means that normally end users do not have the negotiating power to amend or change any boilerplate terms, but only accept all or refrain from using the software.[154] It is thus premature for China to simply follow the current U.S. position under the copyright preemption cases to allow enforcement of these terms. This Article proposes that China should follow the EU position to at least disallow certain limiting terms based on policy considerations. Indeed, allowing unrestricted enforcement of these prohibitory terms disrupts the balance set by current IP laws. Unlimited contract rights combined with IP rights may result in exclusionary overprotection, which overly restricts

---

152 *See supra* Part IV.B.i.

153 *See, e.g.*, Bowers v. Baystate Techs., Inc., 320 F.3d 1317, 1325-26 (Fed. Cir. 2003) ("[C]ase law indicates the First Circuit would find that private parties are free to contractually forego the limited ability to reverse engineer a software product under the exemptions of the Copyright Act.").

154 *See generally* Marotta-Wurgler & Taylor, *supra* note 12 (using software end user licensing agreement, which is a common standard contract, to empirically assess whether these standard contracts change over time).

public use of information and discourages cumulative innovations such as investment in improving programs.[155] Since the software industry largely relies on incremental and cumulative innovations, [156] the one-size-fits-all approach of unrestrictedly enforcing anti-reverse engineering terms is not sound. In addition, the software industry in China is still in a phase that has relatively more needs for referencing and learning for cumulative innovations, compared to the much-developed U.S. software industry. [157] Allowing unlimited enforcement of these terms is not justified in China, considering its significant negative impact on public interests. Therefore, it is more reasonable for China to follow the EU to prevent some types of reverse engineering ends, such as for research, study, and interoperability, from contractual limitations.

Arguing against a wholly friendly approach toward these terms does not mean that the other extreme should be adopted instead. If *Kewanee* and *Bonito* are strictly interpreted and followed, the U.S. patent preemption analysis may strike down all kinds of anti-reverse engineering terms, since they disrupt patent law policy.[158] China, however, should not go to this extreme either. Software program reverse engineering technology has become highly developed, making reverse engineering programs increasingly cheaper and easier.[159] For example, Genshin Impact, a popular open-world game developed by a Chinese company, is easily reverse engineered by players, resulting in the public leakage of much undisclosed information (for example, new characters and new events).[160] In light of this, it seems more reasonable that certain contractual limitations adopted by software companies be enforced. Otherwise, there may be under-protection problems, leading to

---

155 *See* Rice, *supra* note 12, at 557.

156 *See* Samuelson et al., *supra* note 33, at 2330-32; Mahajan, *supra* note 49, at 3327-28.

157 *See* Chen Shan, *supra* note 69, at 241.

158 *See supra* Part IV.B.iii.

159 *See* LaRoque, *supra* note 5, at 439-40.

160 For reverse engineering of this game by players outside China, see *Reverse Engineering Adventures: Brute-force function search, or how to crack Genshin Impact with PowerShell*, KATY'S CODE (Jan. 24, 2021), https://katyscode.wordpress.com/2021/01/24/reverse-engineering-adventures-brute-force-function-search-or-how-to-crack-genshin-impact-with-powershell/ [https://perma.cc/7BJ2-USZC] (offering a guide on how to reverse engineer Genshin Impact). Indeed, reverse engineers will release any new information about the new version of this game far before it is officially released.

underinvestment in innovations.[161] Accordingly, the one-size-fits-all approach, in either extreme position, should not be adopted in Chinese legislation. The more reasonable and optimal approach would lie somewhere between the two extremes. Rejecting this one-size-fits-all approach is consistent with the EU position, which adopts an intermediate approach to maintain a sound private-public interest. [162] Also, if *Kewanee* and *Bonito* are interpreted to accommodate the software industry features, the U.S. patent preemption analysis may support limited contractual bans on reverse engineering, while disallowing a total ban.[163] In light of the U.S. and EU analysis, this Article argues that it is more appropriate for China to adopt an intermediate approach to allow limited contractual bans, while invalidating a total restriction.

b. Toward an Intermediate Approach

Previous discussions have shown that an intermediate approach to allow limited bans on reverse engineering is a more appropriate choice for China. The remaining question is what limited contractual limitations can or cannot be enforced. This largely depends on whether allowing or invalidating bans on particular types of reverse engineering can maintain a sound balance between private rights and public interest. Reverse engineering software programs can be classified into many types. The most frequent and common types include: (1) for pure research and study; (2) to achieve interoperability or compatibility; (3) to develop and market a competing product (imitation); and (4) to develop and market an improved product.[164] It is relatively easier to discuss the contractual limitations on the first two types. First, reverse engineering for personal study and research purposes does not have any impact on the software companies' market. This behavior is limited to reverse engineers' personal use, and it does not produce any new or competing programs. Since this type of conduct does not erode the lead time enjoyed by software companies, there is no justification to allow companies to use contract terms to limit them. Otherwise, the public interest in using the underlying information may be

161 *See* Rice, *supra* note 12, at 557.

162 *See supra* Part IV.C.

163 *See supra* Part IV.B.iii.

164 *See* Rice, *supra* note 12, at 555-56; Mahajan, *supra* note 49, at 3314-15.

excessively disrupted. That is the reason why the EU law disallows companies to limit this conduct through contracts.[165] In this regard, China can follow the EU position. Second, reverse engineering for interoperability or compatibility is economically sound. It promotes interoperability to prevent platform monopolies that harm consumer welfare.[166] That is why the EU law exempts reverse engineering for interoperability and makes it a non-waivable right.[167] Drawing insights from the EU rule and its underlying policy rationales, the Chinese law should also not enforce anti-reverse engineering clauses on interoperability or compatibility.

Regarding reverse engineering to develop and market a competing product (imitation), this can be prohibited by licensing terms freely. Considering the current technology for reverse engineering, if reverse engineers can freely use the information to quickly develop and market a competing or functionally equivalent product, the lead time enjoyed by software companies is significantly eroded. Since reverse engineering costs are decreasing due to the advancement of technology, reverse engineers can charge lower prices when marketing the competitive product, largely eroding the market share of the rights holders. This may negatively impact the creative incentives of rights holders. Therefore, to retain a justifiable private-public balance, it seems more appropriate to allow enforcement of limited contractual restrictions on reverse engineering for direct competition in China, similar to the U.S. position where the analysis of patent preemption, considering software industry features, seems to be more supportive for these limited contractual bans.[168]

The enforceability of contractual bans on reverse engineering to develop and market an improved product is more complicated. For one thing, allowing reverse engineering for producing and marketing an improved product may erode the market share of rights holders, since the improved products can be said to directly compete with the original ones. For another, innovating around the original software programs is not similar to just producing functionally equivalent products. The former adds more to the public welfare, as it provides new and better programs to consumers, although it directly competes with the original program

---

165 *See supra* Part IV.C.

166 *See id.*

167 *See id.*

168 *See supra* notes 140-42 and accompanying text.

developers. The latter does not provide any new products to the public and has an even more critical effect on the marketing of the original programs. That said, it seems that the interest of the original creators and the needs for cumulative innovations are in a deadlock. How the law in China should choose its position depends largely on which interest or need the Chinese law should prioritize. As seen in the United States, the preemption doctrine on the enforceability of anti-reverse engineering clauses should consider industry features.[169] The same is true for China, when deciding whether to allow contractual bans on this kind of reverse engineering. The software industry largely relies on incremental and cumulative innovations to develop.[170] Accordingly, considering this industry feature, it seems more appropriate if the law favors the need for cumulative innovations more, to invalidate any contract bans on reverse engineering for producing improved products. This position is even more appropriate, considering that the Chinese software industry is still not that developed, which requires greater room for cumulative innovations.[171] What makes this position more justified is that, if these contractual bans are not allowed, the original creators may have more incentives to improve their current programs, rather than simply resting on the monopoly rights of their original programs. Therefore, this Article argues against the Chinese law allowing anti-reverse engineering if the pertinent clauses restrict the conduct that leads to product improvement.

c. Summary and Steps Going Forward

Based on the comparative insights from the U.S. and EU laws, this Article argues that the Chinese law should be reformed to incorporate clear provisions to invalidate contractual bans on reverse engineering for research and study, interoperability or compatibility, and innovating around original programs. However,

---

169 *See supra* Part IV.

170 *See supra* notes 136-37 and accompanying text.

171 Although the Chinese software industry has developed very quickly during recent years, it is still not that competitive in the international market compared with other countries such as the Indian software industry. *See* Xiangdong Chen, Ruixi Li, Miaochen Lv, Dian Chen & Lingzi Yang, *Information Technology Industry in China*, *in* INNOVATION, ECONOMIC DEVELOPMENT, AND INTELLECTUAL PROPERTY IN INDIA AND CHINA 71, 81 (Kung-Chuang Liu & Uday S. Racherla eds., 2019).

the private bans on reverse engineering for producing and marketing functionally equivalent programs should be upheld. In addition to these clear provisions, a forward-looking approach should take potential future reverse engineering behaviors into account. Thus, there should be a miscellaneous provision allowing courts flexibility in dealing with contractual bans on reverse engineering for new purposes, based on policy considerations on a case-to-case basis, [172] since there is a possibility that reverse engineers may decompile or disassemble programs for other new purposes in the future. In the short term, these clear provisions plus the miscellaneous provision on the enforceability issue can be included in the Regulation on Computers Software Protection. In the long run, when situations become more mature, these provisions can be incorporated into the PRC Copyright Law or even the Trade Secrets Law (AUCL or its corresponding judicial interpretations), depending on the legislative agenda and process.

VI. CONCLUSION

This Article explored the current intellectual protections for software programs in China and introduced the limits of the exclusive rights software companies frequently use the contract law to remedy. The anti-reverse engineering clause is a typical example of companies' efforts to supplement IP protections for software programs. The enforceability of these terms is a critical issue, which disrupts the balance set by IP laws. The descriptive analysis of the Chinese position on this enforceability issue reveals that significant uncertainty exists in the legal treatment of these terms. Reforms are necessary to alleviate the uncertainty. This Article conducted the comparative analysis by exploring the U.S. and EU positions of this enforceability issue to provide valuable insights and policy implications for our discussions on the Chinese reform suggestions. Ultimately, Chinese law should be reformed to include clear provisions allowing limited contractual bans, but disallowing total bans. Moreover, a miscellaneous provision should be included to fit

---

172 *See* Fei Yanying (费艳颖)& Zhou Wenkang (周文康), *Shangye Mimi Fanxiang Gongcheng De Gongneng, Guanxi Yu Lujing Tanxi*(*商业秘密反向工程的功能、关系与路径探析*) [*Probe Into the Function, Relationship and Path Behind the Trade Secrets Reverse Engineering*], 1 SCI. TECH.& L.(CHINESE-ENG. VERSION) 75 (2021).

in with the rapid development of the software industry and deal with potential future conducts.