DIGITAL REMEDIES

Maayan Perel†

ABSTRACT

Legal disputes increasingly arise on digital grounds in relation to an array of subjects such as online enforcement of intellectual property, the First Amendment and online speech, and the right to privacy in personal data stored on digital devices. When courts are called upon to resolve disputes relating to cyberspace, many of the reliefs they grant are executed by digital means, such as technologies that restrict access to unwarranted content or technical solutions that enable or disable access to digital devices. The essence of digital remedies is their profound technological details, some of which may elude judicial review. Like equitable remedies directed to the physical world, digital remedies are usually open-ended, affording their executors broad discretion on how to implement them. However, unlike physical remedies, the implementation of digital remedies is embedded in inherently non-transparent technologies designed and executed privately outside the courthouse and has a robust, dynamic, and ongoing impact on third-party stakeholders. Digital remedies' technical details may far surpass what the court defines, converting compliance from a technical matter of law enforcement into a substantial matter of law making. Although equitable remedies generally create greater difficulties for courts in ascertaining and ensuring compliance, digital remedies take these concerns to the next level, presenting serious challenges to the rule of law.

This Article argues that the issuance and execution of digital remedies challenges the court's ability to fulfill its longstanding duty to exercise its adjudication power in accordance with rule of law, to competently prescribe remedies that are fit to redress the violation of rights, and to assure these remedies are enforced properly. Using the example of website-blocking injunctions, this Article demonstrates that the devil is in the details of implementing digital remedies. These details play a crucial role in shaping the meaning of digital remedies, and consequently the definition of the rights they purport to vindicate. Overall, the Article recommends several mechanisms that courts can exploit in order to extend their oversight and retain more control over the critical implementation stage of digital remedies. This Article builds on the system of equitable remedies, which includes, in addition to the remedy itself, equitable managerial devices that allow courts to manage the parties and ensure compliance, as well as special equitable restraints. This Article aims to empower judges who resolve cyber-related disputes with a broader and a more accurate understanding of the meaning of their digital solutions.

DOI: https://doi.org/10.15779/Z38RX93D8V

† Assistant Professor, Netanya Academic College; Senior Researcher, Center for Cyber Law and Policy, University of Haifa; S.J.D, University of Pennsylvania School of Law. I would like to thank Eran Bareket, Daniel Benoliel, Dan Burk, Karni Chagal, Peter Drahos, Amit Elazari, Niva Elkin-Koren, Orit Fischman-afori, Nissan Franco, Ellen Goodman, Eldar Haber, Jacob Assaf and Sharon Sandeen for their excellent comments. Special thanks are also due to the participants of the 2018 GIF Young Scientists Meeting at Potsdam, the participants of the 2018 Internet Law Scholars Conference at New York Law School and the participants of the ICIL 2018 Conference at Antwerp University for fruitful brainstorming. This research was supported by the Center for Cyber Law and Policy, University of Haifa. Any mistakes or omissions are the author's.

TABLE OF CONTENTS

I. INTRODUCTION

The impact of digital technology on regulation, law enforcement, and compliance has been investigated extensively.[1] Law and technology

1. *See generally* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553 (1998) (showing that the creation and implementation of information policy are embedded in network designs and standards as well

scholarship explores how governance with the aid of technology challenges fundamental rights and democratic values, such as due process and the rule of law.[2] Prior work argues that the delegation of public powers to private actors using proprietary technology is black-boxed and thus difficult to oversee.[3] Specifically, current literature focuses on *out-of-court* delegations of public powers held by administrative actors, such as credit score providers,[4] regulated firms,[5] police,[6] municipal cities,[7] or online platforms that regulate online

---

as in system configurations); LAWRENCE LESSIG, CODE: VERSION 2.0 (2006); Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669 (2010) (describing private automated law systems that failed to recognize risks to bank capital reported, leading into global financial crisis); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1256 (2008) (describing the Colorado Benefits Management System, which generates welfare eligibility decisions); Maayan Perel & Niva Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, 19 STAN. TECH. L. REV. 473, 477 (2016) (describing internet service provider algorithms); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 673 (2016) (showing how algorithmic techniques like data mining challenge the prohibition of discrimination in employment).

2. *See, e.g.*, Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1 (2005); TARLETON GILLESPIE, WIRED SHUT: COPYRIGHT AND THE SHAPE OF DIGITAL CULTURE 240–42 (2007); Citron, *Technological Due Process*, *supra* note 1, at 1252; Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 J. TELECOMM. & HIGH TECH. L. 235, 235–36 (2011); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014); Perel & Elkin-Koren, *Accountability in Algorithmic Enforcement*, *supra* note 1; Maayan Perel & Niva Elkin-Koren, *Black Box Tinkering: Beyond Transparency in Algorithmic Enforcement*, 69 FLA. L. REV. 181 (2017); Robert Brauneis & Ellen P. Goodman, Note, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 114–15 (2018); Nicholas Diakopoulos, *We Need to Know the Algorithms the Government Uses to Make Important Decisions About Us*, CONVERSATION (May 23, 2016), https://theconversation.com/we-need-to-knowthe-algorithms-the-government-uses-to-make-important-decisions-about-us-57869 [https://perma.cc/U37E-HHKD].

3. FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 8 (2015); Perel & Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, *supra* note 1, at 482; Perel & Elkin-Koren, *Black Box Tinkering*, *supra* note 2, at 183.

4. *See, e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 89 (2014).

5. *See, e.g.*, Bamberger, *Technologies of Compliance*, *supra* note 1, at 673 (contending that government regulators encourage compliance through automation).

6. Walter L. Perry et al., *Predictive Policing: Forecasting Crime for Law Enforcement*, RAND (2013), https://www.rand.org/pubs/research_briefs/RB9735.html [https://perma.cc/T4WZ-NJHK].

7. *See, e.g.*, Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 107 (2018) (describing how the "smart city" movement impresses on local governments the importance of collecting and analyzing data more effectively).

speech,[8] to privately designed systems of automated decision-making.[9] Left largely unaddressed by this work, however, is the privatization of remedial powers ordinarily held by courts. These powers are often outsourced to private parties who employ digital means for compliance purposes.

Judicial remedies increasingly encompass a crucial aspect of algorithmic compliance by private actors. When courts are called upon to resolve disputes relating to cyberspace (everything that relies on interconnected technologies, such as online content or digital devices), many of the reliefs they grant depend on digital implementation by private actors. Restricting access to online content or fixing security flaws in digital devices, for instance, are all done by digital means. Nevertheless, as this Article contemplates, implementation of digital remedies is far from being solely a procedural matter of compliance. It essentially shapes the scope and breadth of the remedy and defines the practical balance between various rights and interests.

The interplay between rights and remedies has been widely explored before.[10] Most notable is the notion that remedies determine the efficacy of rights.[11] But remedies are also known for shaping the meaning of substantive law. Indeed, recent scholarship in public law highlights the importance of thinking carefully about the remedial environments from which substantive law emerges. Though varied in their evaluative approaches and prescriptive contributions, remedies law scholars agree that "remedy-related variables affect not just the intensity with which substantive rights get enforced, but also the defining of substantive rights themselves."[12] This Article contributes to this discourse, contending that the technological details of implementation are a crucial variable in defining the meaning of digital remedies and the rights they vindicate. Therefore, digital remedies demand the close attention of the judiciary.

---

8. Perel & Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, *supra* note 1, at 480–81 (explaining that online intermediaries currently manage and police the usage of online content pursuant to different laws).

9. *See* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 380 (2006).

10. Within individual fields, commentators have drawn attention to the linkage between remedial context and substantive law, and some commentators have proposed targeted responses to particular instances of the phenomenon. *See, e.g.*, Douglas Laycock, *How Remedies Became a Field: A History*, 27 REV. LITIG. 161, 165 (2008); Samuel L. Bray, *The Myth of the Mild Declaratory Judgment*, 63 DUKE L.J. 1091, 1110–13 (2014); Daryl J. Levinson, *Rights Essentialism and Remedial Equilibration*, 99 COLUM. L. REV. 857, 887 (1999); Nancy Leong, *Making Rights*, 92 B.U. L. Rev. 405, 421–75 (2012); Jennifer E. Laurin, *Rights Translation and Remedial Disequilibration in Constitutional Criminal Procedure*, 110 COLUM. L. REV. 1002, 1007 (2010).

11. Michael Coenen, *Spillover Across Remedies*, 98 MINN. L. REV. 1211, 1213 (2014).

12. *Id.* at 1216.

A prime example concerns the cryptographic legal battle between the FBI and Apple regarding the FBI's access to the locked iPhone of one of the San Bernardino terrorists. The FBI requested that the court force Apple to create software to help them defeat the phone's encryption by creating a technological "backdoor" that would allow the government access to the data stored not just on the suspect's device, but also on millions of Apple devices.[13] While the FBI eventually withdrew its motion, choosing instead to use the services of a private third party to break into the phone, a decree forcing Apple to redesign its digital devices could have had dramatic implications for U.S. residents, dissidents, and especially individuals in countries with repressive governments.[14] Indeed, how Apple would have practically designed this "backdoor" would affect the vulnerability of national security networks to penetration by malicious hackers, including ones from other nations.[15] It would have also redefined the scope of freedom of expression.[16] Far-reaching ramifications for collective safety and security would have also resulted from a remedy "weakening cryptography through the creation of mandatory backdoors."[17]

Digital remedies can have a robust impact on the rights of numerous stakeholders. In particular, the *details* of implementing digital remedies shape their substance, transforming compliance from a technical matter of law

---

13. Ron Wyden, *This Isn't About One iPhone. It's About Millions of Them*, WIRED (Feb. 19, 2016, 12:00 AM), https://www.wired.com/2016/02/this-isnt-about-one-iphone-its-about-millions-of-them [https://perma.cc/5E5L-RQJT].

14. *See Amicus Briefs in Support of Apple*, APPLE (Mar. 2, 2016), https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple [https://perma.cc/V6NM-8SAG]; Brief of American Civil Liberties Union et al. as Amici Curiae Supporting Apple, Inc., *In re* Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 3, 2016); Brief of Privacy International and Human Rights Watch as Amici Curiae Supporting Apple, Inc., *In re* Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 3, 2016); Brief of the Center for Democracy & Technology as Amicus Curiae Supporting Apple Inc., *In re* Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 3, 2016); Letter from David Kaye, Special Rapporteur on the Promotion & Prot. of the Right to Freedom of Op. & Expression, United Nations Human Rights Council, to Hon. Sheri Pym (Mar. 2, 2016), https://freedex.org/wp-content/blogs.dir/2015/files/2017/08/Letter_from_David_Kaye_UN_Special_Rapporteur_on_the_promotion_and_protection_of_the_right_to_freedom_of_opinion_and_expression.pdf [https://perma.cc/8FC5-RHVY].

15. Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, *In re* Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (C.D. Cal. Feb. 25, 2016).

16. Brief for International and Human Rights Watch as Amici Curiae Supporting Apple Inc., *In re* Search of an Apple iPhone, No. CM 16-10 (C.D. Cal. Mar. 3, 2016).

17. Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance by Design*, 106 CALIF. L. REV. 697, 725 (2018).

enforcement into a substantive matter of law making. The implementation of digital remedies requires defendants to act as both judge and executor and perform functions that are normally reserved for authorized governmental bodies.[18] Website-blocking injunctions demonstrate this idea perfectly, as they show how focal the technical details of the blocking technique could turn out to be. Such injunctions have been used widely in various jurisdictions throughout Europe.[19] The United States has also recently implemented such an injunction in a default judgment against Sci-Hub, a popular online platform for unauthorized dissemination of scientific scholarship.[20]

Technically, website blocking can be achieved by different means, each of which having its own special attributes. The particular implementation technique applied (whether through Internet Protocol (IP) blocking or URL blocking) ultimately shapes the boundaries of enforcement; it can actually surpass settled law, resetting the effective balance between copyright on the one hand, and free speech, privacy, and access to information on the other, while affecting the rights and interests of numerous internet users.

Overseeing how digital remedies unfold and anticipating their ultimate impact is nonetheless challenging. Remedies that compel action or inaction—that is, equitable remedies—generally create great difficulties for courts in ascertaining and ensuring compliance;[21] digital remedies heighten these issues. Like equitable remedies directed to the physical world, such as ordering a defendant to restore the plaintiff's property to its undamaged condition,[22] digital remedies leave room for flexible implementations.[23] Nevertheless, contrary to the evident, real-world implementation of remedies directed to the physical world, the implementation of digital remedies is generally embedded in proprietary, inherently non-transparent technologies. Additionally, predicting the ultimate reach of digital remedies in advance is extremely challenging, as their efficacy often depends on their ability to adjust promptly to the changing digital landscape. Oftentimes, they are directed to resolve an

18. Perel & Elkin-Koren, *Accountability in Algorithmic Enforcement*, *supra* note 1, at 485.

19. *See generally* MARTIN HUSOVEC, INJUNCTIONS AGAINST INTERMEDIARIES IN THE EUROPEAN UNION (2017).

20. *See* Am. Chem. Soc'y v. Sci-Hub, No. 1:17-cv-726 (E.D. Va. June 23, 2017).

21. Samuel L. Bray, *The System of Equitable Remedies*, 63 UCLA L. REV. 530, 564 (2016) (explaining that defendants might be recalcitrant, unsure how to comply or slow to react; that circumstances may change, and that court orders might be mistaken).

22. *See, e.g.*, Barngrover v. City of Columbus, 739 S.E.2d 377 (Ga. 2013) (describing history of an equitable remedy order in a nuisance case).

23. Bray, *supra* note 21, at 562 ("In contemporary American law the remedies that compel action or inaction are paradigmatically equitable ones. And the remedies that not only compel action or inaction, but also do so in an open-ended and less determinate fashion, are wholly equitable.").

ongoing problem. Blocking injunctions, for instance, can soon become outdated if users and content providers conceal their online conduct by using virtual private networks (VPNs), proxy services, etc. Their efficacy largely depends on their ability to adapt to changing digital circumstances, and this further complicates the ability of courts to oversee how they evolve. But if courts cannot anticipate how digital reliefs unfold, they cannot ensure that they are actually fit to redress specific violations of rights. Ultimately, this challenges the rule of law.

The meaning of digital remedies is defined by their profound technical details which are determined and implemented outside the courthouse, on private grounds, under the veil of algorithmic opaqueness and private considerations. The execution of digital remedies, however, must not be left unchecked. Proper safeguards are necessary to preserve the rule of law and ensure that digital remedies effectively achieve their intended purpose. Otherwise, potential distortions of settled law will avoid judicial review.

Accordingly, the Article proceeds as follows. Part II provides a basic introduction of remedies law. To probe why digital remedies introduce new and intricate challenges for the judiciary, this Part describes the various goals of remedies and describes their fundamental distinctions. Following several examples, it proceeds to classify digital reliefs as specific, prospective, and equitable remedies. Part III uses the example of website-blocking injunctions to demonstrate why the digital details of implementation play such a crucial role in shaping the meaning of digital remedies, and consequently the definition of the rights they purport to vindicate. Next, whether this shift in adjudication power could be adequately dominated by the judiciary is considered in Part IV. Specifically, Part IV addresses how digital remedies challenge the ability of the court to fulfill its longstanding duty to exercise its adjudication power in accordance with the rule of law, to competently prescribe remedies that are fit to redress the violation of rights, and to ensure these remedies are enforced properly. Overall, this Part points at three attributes of digital remedy that impede their predictability. First, their ultimate meaning evolves outside the courthouse. Second, their implementation details are dynamic in their implications, costs, and capabilities of adjusting to the changing digital landscape. And third, these details are embedded in privately-developed, non-transparent codes. Finally, Part V recommends several mechanisms that courts can exploit in order to extend their oversight and retain more control over the critical implementation stage of digital remedies. Particularly, it builds on the system of equitable remedies, which includes, in

addition to the remedy itself, equitable managerial devices that allow courts to ensure compliance, as well as special equitable restraints.[24]

II. THE RISE OF DIGITAL RELIEFS

To probe why digital remedies introduce new and intricate challenges for the judiciary, it is helpful first to gain a general understanding of the law of remedies. This Part explains the various goals of remedies and describes their fundamental distinctions. Following several examples, it proceeds to classify digital reliefs as specific, prospective, or equitable remedies.

A. JUDICIAL REMEDIES

Court decisions end by either granting the plaintiff a relief or otherwise rejecting her request. "Remedies are the means by which substantive law is given its actual effect."[25] Indeed, there is "no right without a remedy."[26] The goals of remedies law are varied. Compensatory damages purport to restore the "plaintiff's rightful position" through monetary transfers between plaintiff and defendant.[27] Preventive remedies, on the other hand, seek to avoid harm, for instance, by enjoining individuals from acting or ordering them to take affirmative steps to thwart the violation of the law.[28] Equitable remedies promote restitution: they are designed to deprive defendants of the benefit of wrongful acts. Remedies could also promote deterrence and morality, for instance, when courts "enhance damages beyond what is necessary to compensate plaintiffs or deprive defendants of profits in order to punish" culpable behaviors.[29]

A core distinction in the law of remedies is the difference between specific and substitutionary relief.[30] While specific reliefs afford the plaintiff the original thing to which she was entitled, substitutionary reliefs afford the plaintiff

---

24. For additional reasons, see Bray, *supra* note 21, at 534.

25. Mark A. Lemley & Bryan Casey, *Remedies for Robots*, 86 U. CHI. L. REV. 1311, 1343 (2019).

26. Frederick Pollock, *The Continuity of the Common Law*, 11 HARV. L. REV. 423, 424 (1898) (noting the phrase already functioned as a "maxim" in the 19th century).

27. DOUGLAS LAYCOCK, MODERN AMERICAN REMEDIES 11–15 (4th ed. 2011).

28. *Id.*

29. Lemley & Casey, *supra* note 25, at 3.

30. *See, e.g.*, DAN B. DOBBS, LAW OF REMEDIES: DAMAGES. EQUITY, RESTITUTION 209 (2d ed. 1993) (distinguishing between substitutionary and specific remedies); JAMES M. FISCHER, UNDERSTANDING REMEDIES 4 (1999) (discussing the distinction between specific and substitutional remedies in section on "Types of Remedies"); DOUGLAS LAYCOCK, THE DEATH OF THE IRREPARABLE INJURY RULE 12–13 (1991) ("The most fundamental remedial choice is between substitutionary and specific remedies.").

something that substitutes for the original thing to which she was entitled.[31] Money is a typical example of the latter.[32] Injunctions are a typical example of the former;[33] they are considered specific reliefs because they either direct or restrain the defendant's actions.[34] The idea is that an injunction, such as one ordering the defendant to stop selling counterfeit goods, intends to prevent ongoing or future violations of the plaintiff's legal entitlement (ownership of intellectual property, in this example). Similarly, mandamus, ejectment, replevin, and specific performance are also considered specific remedies because they purport to give the plaintiff the original thing or condition to which she was entitled.[35]

To grant a specific relief, the court must first define the borderline of the plaintiff's entitlement, or in other words, the scope of the legal right that was violated. This depends on the court's specific approach regarding the nature of the substantive law. A "normative" approach, which is consistent with laws enforced by property rules,[36] views the substantive law as a prohibition against certain conduct, and thus seeks to stop the wrongful act or to compensate the plaintiff for the damage done.[37] An "economic" approach, which is consistent with laws enforced by liability rules, holds that the substantive law "merely specifies the foreseeable consequences of various choices."[38] Under this approach, remedies essentially signal the costs of doing business.[39] When granting a substitutionary relief, courts have to evaluate the plaintiff's loss and then design a substitute equal to the value of her original entitlement.[40]

---

31. Colleen P. Murphy, *Money as "Specific" Remedy*, 58 ALA. L. REV. 119, 120 (2006).

32. *Id.* ("[T]he defendant has violated a legal entitlement belonging to the plaintiff—such as a personal, proprietary, dignitary, or economic entitlement—and the court awards money for the resulting harm."). Of course, money might also be a specific remedy; for instance, when the plaintiff's original entitlement is monetary (and the defendant fails to pay what he owes to the plaintiff).

33. Although injunctions could arguably be also substitutionary (for instance, when they provide a thing or condition other than the plaintiff's original entitlement). *See* Charles Alan Wright, *The Law of Remedies as a Social Institution*, 18 U. DETROIT L.J. 376, 378 (1955).

34. *See, e.g.*, Larson v. Domestic & Foreign Commerce Corp., 337 U.S. 682, 688 (1949).

35. Murphy, *supra* note 31, at 123.

36. *See generally* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972) ("An entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller.").

37. Lemley & Casey, *supra* note 25, at 44.

38. *Id.*

39. *See* Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027, 1033 (1995); *see also* Louis Kaplow & Steven Shavell, *Do Liability Rules Facilitate Bargaining? A Reply to Ayres and Talley*, 105 YALE L.J. 221, 222 (1995).

40. Laycock, *supra* note 30, at 13.

Another remedial distinction is between prospective and retrospective relief. Prospective relief refers to "remedies that prevent wrongful conduct or that prevent the post-judgment accrual of harms flowing from the defendant's pre-judgment conduct."[41] Retrospective relief refers to "remedies for harms that have accrued up to the date of judgment."[42] Oftentimes (but not always), prospective remedies will be specific reliefs because they will usually afford the plaintiff the original thing to which she is entitled.[43] Retrospective reliefs, on the other hand, will usually (but again, not always) be substitutionary, namely awarding money for physical harm caused by the defendant.[44]

Finally, a longstanding dichotomy in remedies law, which is also the most suitable to address digital remedies as explained henceforth, is the one that differentiates between legal and equitable remedies. This historical classification is essentially evaluated by asking whether a given remedy was available in courts of law or courts of equity.[45] The most common remedy in the courts of law was money, whereas the most common remedy in the courts of equity was the personal order to act in a specific manner or refrain from acting in some way, such as with orders of specific performance or injunctions.[46] Accordingly, equitable remedies are granted "to compel action (or inaction), especially when that action may be continuing or iterative and not easily measured."[47] The available equitable remedies are the injunction, specific performance, reformation, quiet title, and various "restitutionary remedies: accounting for profits, constructive trust, equitable lien, subrogation, and equitable rescission."[48] The legal remedies mainly include "damages, mandamus, habeas, replevin, ejectment, and certain restitutionary remedies."[49]

A standard view among American scholars is that the distinction between legal and equitable remedies is outmoded.[50] Modern courts treat equitable remedies as specific remedies and legal remedies as substitutionary ones,

41. Murphy, *supra* note 31, at 137.
42. *Id.*
43. *Id.*
44. *Id.*
45. *Id.* at 134–35.
46. *Id.* at 135.
47. Bray, *supra* note 21, at 533.
48. *Id.* at 541–42.
49. *Id.* at 542.
50. Doug Rendleman, *The Trial Judge's Equitable Discretion Following* eBay v. MercExchange, 27 REV. LITIG. 63, 97 (2007); Caprice L. Roberts, *The Restitution Revival and the Ghosts of Equity*, 68 WASH. & LEE L. REV. 1027, 1033, 1060 (2011); *see also* James Steven Rogers, *Restitution for Wrongs and the Restatement (Third) of the Law of Restitution and Unjust Enrichment*, 42 WAKE FOREST L. REV. 55, 56 (2007) (calling distinctions between legal and equitable restitution "little short of gibberish").

although some remedies law scholars contest that such a treatment is inaccurate.[51] Classifying digital remedies as equitable ones is nonetheless important because equitable remedies afford courts with special managerial tools which enable them to better manage the enforcement of equitable remedies.

B. THE SYSTEM OF EQUITABLE REMEDIES

Equitable remedies are not just about compelling action or inaction. A core distinction of equitable remedies relates to their open-ended and ongoing nature. This makes them far less determinate than other outcome-specific, one-shot remedies, such as damages. Consequently, equitable remedies may give rise to a serious problem of compliance.[52] Specifically,

> [s]ome defendants will be recalcitrant, refusing to comply. Others will be ignorant or unsure exactly how to comply. Still others may slow their pace, dragging things out, even if they would not refuse a clear order. Nor does the fault always lie with the defendant. There will be circumstances that the court could not foresee, or at least did not foresee, when it gave the order compelling action or inaction. There will be judicial mistakes, impossibilities, and absurdities.[53]

While assessing compliance with legal remedies is rather straightforward—the actual payment of damages, the moment a prisoner is released from custody, or when property is being replevied and returned—it could be relatively challenging to determine full compliance with equitable remedies. For example, prohibiting a former employee of a pizza parlor from "using, divulging, and communicating to anyone else any of the trade secrets or confidential information" about the pizza parlor's sauce requires ongoing avoidance from the part of the former employee.[54] Whether this injunction is fully complied with or not largely depends on the degree and scope of the employee's cooperation.

The law of equitable remedies, hence, offers a mechanism for managing compliance. This mechanism includes several managerial doctrines that improve the courts' ability to ensure better enforcement of equitable remedies. Part V discusses these doctrines in breadth; thus, for now it is sufficient to

---

51. Murphy, *supra* note 31, at 135.

52. Bray, *supra* note 21, at 563.

53. *Id.*

54. 205 Corp. v. Brandow, 517 N.W.2d 548, 552 (Iowa 1994). For more examples, see Bray, *supra* note 21, at 563–64.

mention them generally: (1) ex-post revision; (2) contempt; (3) equitable helpers; (4) flexibility; and (5) judicial decision-making.[55]

The exploitation of these managerial devices, especially ex-post revision, contempt, and equitable helpers, can be notably costly. Indeed, "the direct and indirect costs of complying with the court's command and the possibility of an afterlife in which that command is clarified, modified, enforced, or dissolved" could be substantial.[56] Therefore, the system of equitable remedies also provides safety valves that purport to prevent their misapplication. These include the doctrine of ripeness, requirements for specificity, and the equitable defenses of laches and unclean hands that are available for defendants.[57] A detailed discussion of these constraining measures and their application to digital remedies is provided in Part VI.

C. CLASSIFYING DIGITAL RELIEFS

Aspects of our everyday conduct are increasingly becoming digital.[58] Technology is embedded so deeply in human lives that in many cases, there is no other way to govern human behavior than to interact with the technologies that shape it.[59] Criminal enforcement, for example, often depends on the police having access to digitally stored data;[60] preventing terrorists from unleashing terror depends heavily on online intermediaries monitoring inciting content;[61] data security builds on applications' developers addressing security flows in their smart devices.[62]

---

55. *See infra* Part V.

56. Bray, *supra* note 21, at 577.

57. *Id.* at 578–86.

58. Rob Kitchin, *Thinking Critically About and Researching Algorithms* 7 (The Programmable City, Working Paper No. 5, 2014), http://ssrn.com/abstract=2515786 [https://perma.cc/4ZAW-U55G]; Jeff Fuhriman, *The Personalization and Optimization of the Internet of Things*, ADOBE BLOG (July 14, 2015), https://theblog.adobe.com/the-personalization-and-optimization-of-the-internet-of-things/ [https://perma.cc/FA7J-J222].

59. Mulligan & Bamberger, *Saving Governance by Design*, *supra* note 17, at 701.

60. For a comparative analysis about government's access to personal data, see generally Ira S. Rubinstein, *Systematic Government Access to Personal Data: a Comparative Analysis*, 4 INT'L DATA PRIVACY L. 96 (2014).

61. Jen Kirby, *Zuckerberg: Facebook Has Systems to Stop Hate Speech. Myanmar Groups: No, it Doesn't.*, VOX (Apr. 6, 2018), https://www.vox.com/2018/4/6/17204324/zuckerberg-facebook-myanmar-rohingya-hate-speech-open-letter [https://perma.cc/CK9K-GC93].

62. Fed. Trade Comm'n v. D-Link Corp., No. 3:17-CV-00039 (N.D. Cal. Sept. 19, 2017) (bringing request for permanent injunction and other equitable relief). The Federal Trade Commission (FTC) brought this complaint against a Taiwanese corporation, D-Link, which develops and sells, among other things, IP cameras that enable customers to monitor private areas of their homes or business. FTC's basic argument is that D-Link has failed to take reasonable steps to protect their routers and IP cameras from widely known and reasonably

With technology playing such a central role in our lives, it is not surprising that many legal disputes, in various legal contexts, including intellectual property, First Amendment and online speech,[63] the right to privacy in personal data,[64] and the right to non-discrimination,[65] are cyber-related, and hence largely dependent on digital resolution. As such, digital reliefs can only be enforced by digital means, although their implications may extend to the physical world, as well.[66] Digital reliefs typically take the form of injunctions and therefore they could be generally characterized as specific, prospective remedies. Most often they are open-ended, setting an ongoing outcome which may be achieved through various digital means. Thus, they could also fall neatly into the category of equitable remedies. What is it, then, that makes them different? To answer this question, let's explore two examples of digital remedies.

TickBox TV, LLC was a distributor of a small Roku-style device that allows users to perform many computer functions on their television set or other monitor, including browsing the internet and streaming media content through various applications that are preloaded by TickBox or later downloaded by users. In a complaint filed by prominent copyright holders in the motion picture industry, plaintiffs alleged that the device's user interface contained

---

foreseeable software security flows, and by failing to do so it violated section 5(a) of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." *Id.* The FTC requires the court to enter a permanent injunction to prevent future violations of the FTC Act by D-Link. This case is still standing in front of a district court in California, but to the extent that the court will grant the order requested, it is possible that it will require D-Link to take technological steps to address the security flows identified by the FTC.

63. Sandvig v. Sessions, 315 F. Supp. 3d 1, 8 (D.D.C. 2018) (arguing that the access section of the Computer Fraud and Abuse Act (CFAA) would criminalize a group of researchers' research activities, which are conducted as a response to new trends in real estate, finance, and employment transactions, which increasingly have been initiated on the internet. As part of their research activities, they wish to find out if automated transactions in these fields are discriminatory. One way to determine whether members of protected classes are being discriminated against is to engage in "outcomes-based audit testing," which involves accessing a website or other network service repeatedly, generally by creating false or artificial user profiles, to see how websites respond to users who display characteristics attributed to certain classes. These activities will violate certain website Terms of Service, and hence could amount to unauthorized access to a computer, violating the CFAA).

64. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019). This case, which was recently decided in favor of hiQ, involved the use of bots by hiQ to scrape data from LinkedIn website in order to create services that alerts employers about their employees' online activity. LinkedIn argued that hiQ violated the privacy of its users, but the court of appeals affirmed the district court's preliminary injunction prohibiting LinkedIn from blocking hiQ from accessing its website.

65. *See Sandvig*, 315 F. Supp. 3d at 8–9.

66. For instance, a court order requiring a supplier of digital home cameras to address specific security flaws and make his camera more protected may reduce house break-ins.

links to applications that provided access to unauthorized streaming versions of their copyrighted works.[67]

In its initial order issued on January 30, 2018, the California Central District Court ordered TickBox to maintain the current version of its software, which had the pre-loaded infringing applications removed. Additionally, the court refused to order TickBox to remove the already-downloaded offending applications from its users' devices, explaining that such an order raised outstanding questions that had to be answered by the parties. Interestingly, the court directed its outstanding questions to the parties, ordering them to "negotiate and attempt to reach agreement upon a stipulated preliminary injunction that will supersede the Court's initial preliminary injunction order."[68]

Subsequently, on February 13, 2018, the court granted another order in the case:

> TickBox shall issue an update to the TickBox launcher software to be automatically downloaded and installed onto any previously distributed TickBox TV device and to be launched when such device connects to the internet. Upon being launched, the update will delete the Subject Software downloaded onto the device prior to the update, or otherwise cause the TickBox TV device to be unable to access any Subject Software downloaded onto or accessed via that device prior to the update.[69]

Ordering TickBox to perform a software update that removes all pre-loaded applications from its users' devices is a digital remedy. It is an open-ended injunction which sets a specific, prospective outcome to be achieved—that TickBox's launcher software will not include or provide applications that link to copyright-infringing websites—but without imposing limitations on the digital means for achieving this outcome. As stressed in the second order, a software update that achieves the desired outcome may either *delete* the problematic apps or *block* the devices' access to these apps. As expanded in Parts III and IV, restricting users' access to content can be accomplished by varied technological means that differ in their cost, scope, and accuracy. Placing such broad discretion to choose how to block the devices' access to allegedly infringing apps in the hands of a private, profit-maximizing defendant

67. Universal City Studios Prods. L.L.L.P. v. TickBox TV L.L.C., No. CV 17-7496-MWF (ASX) (C.D. Cal. Oct. 13, 2017).

68. Universal City Studios Prods. L.L.L.P. v. TickBox TV L.L.C., No. CV 17-7496-MWF (ASX) (C.D. Cal. Jan. 30, 2018) [hereinafter TickBox 1].

69. Universal City Studios Prods. L.L.L.P. v. TickBox TV L.L.C., No. 2:17-cv-07496-MWF (AS) (C.D. Cal. Feb. 13, 2018) [hereinafter Tickbox 2].

makes it difficult for the court to ensure that the relief, as it ultimately unfolds, is adequately tailored to redress the infringement of plaintiff's rights.

The famous battle between the FBI and Apple presents another interesting example of digital remedies. Following the massacre of fourteen people in California at San Bernardino's Inland Regional Center in December 2015, the FBI sought access to the murderer's iPhone. Apple refused to assist the FBI in breaking into the locked phone, so the FBI sought the court's intervention.[70] Relying on the ancient All Writs Act,[71] Magistrate Judge Sheri Pym of the Central District of California issued an order compelling Apple to assist law enforcement agents in decrypting the locked phone.[72] Interestingly, Judge Pym also set forth a recommended technological roadmap describing the specific steps to be taken in order to achieve this outcome.[73] At the same time, the judge allowed Apple to use "alternate technological means from that recommended by the government," as long as the government concurred and these means achieved the functions designated in the order, as well as the functionality described in the technological roadmap provided by the court.[74] In the end, the FBI did not have to enforce this order because a private, external technology company successfully circumvented Apple's security lock and enabled access into the iPhone.[75] Nevertheless, this order remains an excellent example of a digital remedy that is far more specific in its language, although it still remains open-ended in its nature.

These two examples demonstrate that digital reliefs are essentially remedies that compel a specified digital outcome, and therefore they could be generally classified as specific, prospective, and equitable remedies. Digital reliefs are open-ended in varied degrees, leaving the issue of implementation to the defendant's discretion. But this is not new in the realm of equitable remedies. In fact, employing privately-developed technology to redress violations of individual rights is quite prevalent, especially in the areas of environmental law

---

70. Government's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search at 16–18, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 10-16 (C.D. Cal. Feb. 19, 2016).

71. All Writs Act, 28 U.S.C. § 1651(a) (2012).

72. Order Compelling Apple Inc. to Assist Agents in Search, No. ED 15-0451M, *In re* Search of an Apple iPhone (C.D. Cal. Feb. 16, 2016).

73. *Id.* at 3, 4.

74. *Id.*

75. Laura Hautala & Shara Tibken, *FBI to Apple: We Don't Need your iPhone Hack*, CNET (Mar. 21, 2016), https://www.cnet.com/news/fbi-v-apple-we-dont-need-your-iphone-hack/ [https://perma.cc/UYG9-PT8K].

and consumer protection law.[76] What makes digital reliefs different relates to the characteristics and merits of the *digital means* that implement them: as explained and demonstrated henceforth, the digital means executed to implement digital remedies effectively shape their substantial meaning. With digital remedies, *implementation* defines the scope and breadth of the remedies in an incomparable way. Using the example of website-blocking injunctions, the following Part shows how the implementation of digital remedies is far beyond a technical issue of compliance, and therefore should not be left to out-of-court, unchecked management.

III. DIGITAL REMEDIES: WHEN MEANS DEFINE MEANING

In adjudicating claims for relief, courts often proceed in two stages. First, they determine whether a violation of the law has occurred. If so, they next decide whether to grant the requested relief.[77] Formally, these stages are separated. That is, the law of remedies operates independently of the substantive law.[78] Practically, however, remedial law often interacts with rights-based law in many respects. One important interaction relates to enforcement: a right without a remedy is "existent and identifiable, but of limited practical use to its purported beneficiaries."[79] Furthermore, remedial law may shape the meaning of the substantive law: for instance, when a court's ruling on the merits stems from the way it anticipates "the remedial consequences of a legal violation."[80] Additionally, remedies may affect the incentives of litigants to advance particular substantive claims, or "trigger cognitive biases within the judges evaluating these claims."[81]

It is not surprising, then, that this right-remedy interdependence attracts the attention of public law scholars.[82] Underlying this scholarship is "the basic premise that remedy-related variables affect not just the intensity with which substantive rights get enforced, but also the defining of substantive rights themselves."[83] Digital remedies take this premise several steps forward: they

---

76. For instance, where defendants are required to reduce their polluting disposals; or where product developers are compelled to make their products safer.

77. *See, e.g.*, Marbury v. Madison, 5 U.S. 137, 154 (1803) (asking first, "[h]as the applicant a right to the commission he demands?" and asking second, "[i]f he has a right, and that right has been violated, do the laws of his country afford him a remedy?").

78. Coenen, *supra* note 11, at 1213.

79. *Id.*

80. *Id.* at 1213–14.

81. *Id.* at 1215.

82. *See supra* note 10.

83. Coenan, *supra* note 11, at 1216.

show that it is not only the prescription of remedies that impacts the substantive law, it is also—and often more so—the subsequent, out-of-court implementation of digital remedies. Digital reliefs can be implemented through various means that differ very substantially from one another: the *details* of implementation shape the *substance* of the remedy and determine its impact on numerous stakeholders in an unprecedented way.

The following discussion uses website-blocking injunctions to demonstrate why the digital details of implementation play such a crucial role in shaping the meaning of digital remedies, and consequently the definition of the rights they purport to vindicate. In fact, the need to choose between significantly different enforcement methods transforms implementation into an issue of law-making. Whether this shift in adjudication power could be adequately overseen by the judiciary demands careful consideration, as subsequently explained in Part IV.

A. WEBSITE-BLOCKING INJUNCTIONS—BASIC INTRODUCTION

A major objective of cyberlaw is to regulate illegal content online.[84] One of the greatest challenges in this respect is to ensure prompt and efficient enforcement where acting directly against the primary speakers "has proven to be 'heavy-handed, disproportionate, and ineffective.' "[85] Indeed, direct users often conceal their identity behind anonymous user names, complicating the ability to act directly against them.[86] Additionally, illegal content may originate from places outside of the jurisdiction's reach, further complicating enforcement.[87] While "bringing actions against individual users is expensive . . . regulating access via intermediaries is more cost-effective."[88] Therefore, "the liability of [i]nternet intermediaries, particularly Internet Service Providers

84. *See, e.g.*, HANNIBAL TRAVIS, CYBERSPACE LAW: CENSORSHIP AND REGULATION OF THE INTERNET (2013).

85. Christophe Geiger & Elena Izyumenko, *The Role of Human Rights in Copyright Enforcement Online*, 32 AM. U. INT'L L. REV. 43, 44 (2016).

86. *Id.*

87. *See, e.g.*, *Discussion Paper: Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain*, ICC BUSINESS ACTION TO STOP COUNTERFEITING AND PIRACY 74 (Mar. 2015), https://iccwbo.org/content/uploads/sites/3/2015/03/ICC-BASCAP-Roles-and-Responsibilities-of-Intermediaries.pdf [https://perma.cc/T376-AUME] (noting that "[o]ne of the main challenges is addressing both counterfeiting and piracy from websites based outside the jurisdiction in which the infringement takes place").

88. David Lindsay, *Website Blocking Injunctions to Prevent Copyright Infringement: Proportionality and Effectiveness*, 40 U. NEW S. WALES L.J. 1507, 1507 (2017); Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 662 (2003).

('ISPs'), for the unlawful online actions of third party users is a persistent theme" of the content moderation discourse.[89]

Indeed, online intermediaries are becoming a focal point of content moderation.[90] They may enable or disable access by removing or blocking controversial content, or by terminating users' accounts altogether. "Imposing liability on intermediaries can, however, have significant unwelcome effects, or 'collateral damage,' especially on the rights to freedom of expression and privacy of end-users."[91] Indeed, making platforms legally liable for content posted by users could chill free speech and stifle the development of the internet industry.[92]

The most recent addition to intermediary liability law is the prerogative to award injunctions against intermediaries to block internet access (that is, use digital means) in order to prevent online infringements of intellectual property rights. Such injunctions are directed to private intermediaries that are not direct parties to the legal dispute, but presumably have the technological ability to resolve it.[93] They have been used, quite extensively, in Europe.[94] In *Google Inc.*

---

89. *Id.* at 1507.

90. Niva Elkin-Koren & Maayan Perel, *Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law*, OXFORD HANDBOOK OF INTERMEDIARY LIABILITY ONLINE (Apr. 2019), https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780190900571.001.0001/oxfordhb-9780190900571-e-9 [https://perma.cc/U6BK-HRN8].

91. Lindsay, *supra* note 88, at 1507.

92. Zeran v. AOL, Inc., 129 F.3d 327, 331, 335 (4th Cir. 1997); Niva Elkin-Koren, *After Twenty Years: Revisiting Copyright Liability of Online Intermediaries*, *in* THE EVOLUTION AND EQUILIBRIUM OF COPYRIGHT IN THE DIGITAL AGE 29 (Susy Frankel & Daniel J Gervais eds., 2014).

93. MARTIN HUSOVEC, INJUNCTIONS AGAINST INTERMEDIARIES IN THE EUROPEAN UNION (2017).

94. Geiger & Izyumenko, *supra* note 85, at n. 65; *see, e.g.*, Althaf Marsoof, *The Blocking Injunction—A Critical Review of Its Implementation in the United Kingdom within the Legal Framework of the European Union*, 46 INT'L REV. IP & COMPETITION L. 632, 656 (2015). See, for example, in the UK: Twentieth Century Fox Film Corp. & Ors v. British Telecomms. Plc [2011] EWHC 1981 (Ch); EMI Records Ltd. & Ors v. British Sky Broad. Ltd. & Ors [2013] EWHC 379 (Ch); Cartier Int'l AG & Ors v. British Sky Broad. Ltd. & Ors [2014] EWHC 3354 (Ch); Cartier Int'l Ltd. & Anor v. British Telecomms. Plc & Ors [2016] EWHC 339 (Ch). See, for example, in Denmark: Maritime and Commercial Court in Copenhagen, Fritz Hansen A/S and Others v. Telia Danmark, no. A-38-14, transcript from the record of judgments, p. 10 (Dec. 11, 2014), http://kluwercopyrightblog.com/wp-content/uploads/sites/49/2015/01/IA11122014EN.pdf [https://perma.cc/9GMC-BRQ3]. See, for example, in Germany: German Federal Supreme Court of Justice (Bundesgerichtshof), I ZR 3/14, 26 November 2015, DE:BGH:2015:261115UIZR3.14.0. For examples in France, see SCPP v. Orange, High Court of Paris (Tribunal de Grande Instance de Paris), 3rd chamber, Free, SFR et Bouygues Télécom, no. 14/03236, at 7 (Dec. 4, 2014), http://www.legalis.net/spip.php?page=jurisprudence decision&id_article=4386 [https://perma.cc/ZD7C-AX4V] [French]; CJEU, Judgment in

v Equustek Solutions Inc., the Canadian Supreme Court held that it had power, under its general equitable jurisdiction, to grant an injunction against Google, a non-party to the underlying action, to cease indexing or referencing search results that would provide access to a website involved in intellectual property infringement.[95]

In the United States, however, website blocking seems to clash with the deeply rooted regime of safe harbor. In the early days of the internet, online companies and policymakers feared that making platforms legally liable for content posted by users would chill free speech and stifle the development of the internet. Hence, to mitigate such a threat, legislatures limited the liability of sites that hosed digital content for harm caused by their users (safe harbor). The safe harbor provisions of the Digital Millennium Copyright Act (DMCA)[96] and Section 230 of the Communications Decency Act[97] are intended to protect the democratic nature of the internet and prompt diversity and participation in the online sphere. They are still considered by many as "the most influential law[s] to protect the kind of innovation that has allowed the [i]nternet to thrive . . . ."[98] Accordingly, intermediaries are free to facilitate users' exchange

---

UPC Telekabel Wien, C-314/12, EU:C:2014:192 (Mar. 27, 2014); ECtHR, Akdeniz v. Turkey (dec.), no. 20877/10 (Mar. 11, 2014).

95. Google Inc. v. Equustek Solutions Inc., [2017] 1 S.C.R. 824 (Can.). In this landmark decision released recently by the Supreme Court of Canada, the court upheld the lower courts' decision ordering Google to de-index all websites selling goods that violated a Canadian company's trade secrets worldwide. *Id.* Equustek is a small Canadian technology company whose intellectual property was infringed by Datalink, a former distributer of Equustek's products. *Id.* Equustek brought an action against Datalink and obtained court orders prohibiting the sale of inventory and the use of Equustek's intellectual property. *Id.* Nevertheless, Datalink left Canada and continued offering the infringing products from an unknown location. *Id.* Google had subsequently de-indexed 345 specific webpages associated with Datalink; however, since it did not de-index entire websites and it limited the de-indexing to searches conducted on google.ca, this voluntary step was ineffective. *Id.* Datalink simply moved the objectionable content to new pages within its websites, circumventing the court orders. *Id.* As a result, Equustek obtained an interlocutory injunction to enjoin Google from displaying any part of Datalink's websites on any of its search results worldwide. *Id.* Subsequently, the U.S. District Court of Northern California granted Google a temporary injunction blocking the enforceability of the Supreme Court of Canada's order in the United States, reasoning that Google was protected as a neutral intermediary under Section 230 of the Communications Decency Act 1996. Google L.L.C. v. Equustek Sols. Inc., No. 5:17-CV-04207-EJD (N.D. Cal. Nov. 2, 2017).

96. 17 U.S.C. § 512(a)–(d), (i).

97. 47 U.S.C. § 230.

98. *CDA 230: The Most Important Law Protecting Internet Speech*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230 [https://perma.cc/69S2-MD6S] (last visited Jan. 4, 2020); *accord* Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2313 (2014) ("Section 230 immunity and, to a lesser extent, § 5l2 safe harbors have been

of information without worrying about exposing themselves and their investors to legal risks, and this might include content-blocking obligations.[99]

In relation to intellectual property-related blockings, two anti-piracy bills introduced in 2011, the Stop Online Piracy Act (SOPA)[100] and its Senate counterpart, the Protect IP Act (PIPA),[101] which would purportedly enable courts to issue blocking orders against blacklisted pirate websites, were successfully defeated, following a powerful public protest.[102] The core argument raised by the bills' opponents was that affording law enforcement agents with unprecedented power to create blacklists of illegitimate websites and request the court to compel various internet services to censor them, even though no court had previously found that these services infringed copyright, would disproportionally chill protected speech, given that laws and procedures are already in place for taking down infringing websites.[103]

Nevertheless, a recent case decided by a Virginia district court, *ACS v. Sci-Hub*,[104] may signal a shift in the judiciary's attitude to website blocking.[105] The next Section provides a brief description of the dispute, followed by a discussion of the digital relief granted.

---

among the most important protections of free expression in the United States in the digital age."); David Post, *A Bit of Internet History, or How Two Members of Congress Helped Create a Trillion or So Dollars of Value*, WASH. POST: VOLOKH CONSPIRACY (Aug. 27, 2015), http://wapo.st/1K9AmTh [https://perma.cc/8253-LYWL].

99. Hassell v. Bird, 420 P.3d 776, 778 (Cal. 2018) (ruling that Yelp cannot be forced to remove a review posted on its website since such a removal order improperly treats Yelp as the publisher or speaker of information provided by another information content provider).

100. Stop Online Piracy Act of 2011, H.R. 3261, 112th Cong. (2011).

101. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property (Protect IP) Act of 2011, S. 968, 112th Cong. (2011).

102. Yafit Lev-Aretz, *Copyright Lawmaking and Public Choice: From Legislative Battles to Private Ordering*, 27 HARV. J.L. & TECH. 203, 204–07 (2013).

103. *SOPA/PIPA: Internet Blacklist Legislation*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/coica-internet-censorship-and-copyright-bill [https://perma.cc/PS9P-D5KU] (last visited Jan. 4, 2020).

104. Proposed Findings of Fact and Recommendations, Am. Chem. Soc'y v. Sci Hub, No. 1:l7-cv-0726-LMB-JFA (E.D. Va. Sept. 28, 2017) [hereinafter Magistrate Judge's Proposed Findings].

105. *See* Mitch Stoltz, *Another Court Overreaches With Site-Blocking Order Targeting Sci-Hub*, ELECTRONIC FRONTIER FOUND. (Nov. 10, 2017), https://www.eff.org/deeplinks/2017/11/another-court-overreaches-site-blocking-order-targeting-sci-hub [https://perma.cc/BR9K-CUBX].

B. THE SCI-HUB CASE

Sci-Hub is a well-known website that makes research papers that are normally behind paywalls free to access.[106] Sci-Hub states that its mission is to provide "free access to scientific literature," hosting "more than 58 million peer-reviewed scientific articles for free download."[107] According to a recent study, Sci-Hub provides greater coverage of toll access scholarly articles than the University of Pennsylvania.[108] On June 23, 2017 the American Chemical Society (ACS) sued Sci-Hub for copyright and trademark infringement. ACS contended that "in order to lure users to its illegitimate sources of the Society's stolen content, Sci-Hub conspirators most recently created 'spoofed' websites that mirror the look and feel of the Society's own scientific publishing website."[109]

As happened in a previous copyright suit brought against Sci-Hub,[110] the person behind the website, Alexandra Elbakyan, who operated the site out of Russia using various domain names and IP addresses, did not appear to defend Sci-Hub in court.[111] The Computer & Communications Industry Association (CCIA),[112] however, submitted a brief as amicus curiae, objecting to some portion of the injunction sought by ACS.[113] On November 3, 2017, the court

---

106. SCIENCE HUB, https://sci-hub.tw/ [https://perma.cc/VB8P-R3LJ] (last visited Jan. 4, 2020).

107. Magistrate Judge's Proposed Findings, *supra* note 104.

108. Daniel S. Himmelstein et al., *Research: Sci-Hub Provides Access to Nearly All Scholarly Literature*, ELIFE (Feb. 9, 2018), https://doi.org/10.7554/eLife.32822 [https://perma.cc/AHX6-A25R].

109. *American Chemical Society Files Suit Against Sci-Hub*, AM. CHEMICAL SOC'Y (June 28, 2017), https://www.acs.org/content/acs/en/pressroom/newsreleases/2017/june/acs-files-suit-against-sci-hub.html [https://perma.cc/C3GL-DZXH].

110. Quirin Schiermeier, *US Court Grants Elsevier Millions in Damages from Sci-Hub*, NATURE (June 22, 2017), https://www.nature.com/news/us-court-grants-elsevier-millions-in-damages-from-sci-hub-1.22196 [https://perma.cc/WST8-CVL2].

111. Diana Kwon, *American Chemical Society Wins Lawsuit Against Sci-Hub*, SCIENTIST (Nov. 7, 2017), https://www.the-scientist.com/news-opinion/american-chemical-society-wins-law-suit-against-sci-hub-30648 [https://perma.cc/A8JM-S9D3].

112. The CCIA represents more than twenty large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and internet products and services—companies that provide online services to billions of people around the world.

113. CCIA urged the court to reject the Magistrate Judge's recommendation, insofar as it would extend a permanent injunction in this case to online intermediaries that are not direct parties to the dispute, including internet search engines, web hosting services, and ISPs and require them to "cease facilitating access to any or all domain names and websites through which Defendants engage in unlawful access to, use, reproduction, and distribution of the ACS Marks or ACS's Copyrighted Works." Brief of CCIA as Amicus Curiae Supporting

issued a default judgment ordering Sci-Hub to stop distributing ACS content and imitating its trademark. Furthermore, the court also ruled that

> any person or entity in privity with Sci-Hub and with notice of the injunction, including any Internet search engines, web hosting and Internet service providers, domain name registrars, and domain name registries, cease facilitating access to any or all domain names and websites through which Sci-Hub engages in unlawful access to, use, reproduction, and distribution of the ACS's trademarks or copyrighted works.[114]

Additionally, ACS was awarded $4.8 million in damages.[115]

Such a broad, open-ended injunction is most exceptional in the landscape of remedies law.[116] Opponents of this injunction argued that requiring third parties to censor a pirate website may over-burden innocent actors, who merely provide basic services without encouraging illegal activity.[117] On a procedural level, this may overstep the limits of Rule 65 of the Federal Rules of Civil Procedure, which is extremely strict regarding the specific circumstances under which non-parties to a legal dispute may be enjoined.[118] Indeed, the main argument of CCIA in its amicus brief was that the broad language of the injunction could "sweep in various Neutral Service Providers, despite their having violated no laws and having no connection to this case,"[119] without giving them an opportunity to be heard as required under due process.[120]

Objections to Magistrate Judge's Proposed Findings of Fact and Recommendations at 1, Am. Chem. Soc'y v. Sci-Hub, No. 1:17-cv-0726-LMB-JFA (E.D. Va. Oct. 12, 2017) [hereinafter CCIA Amicus Brief].

114. Magistrate Judge's Proposed Findings, *supra* note 104, at 14–15.

115. Am. Chem. Soc'y v. Sci-Hub, No I: l 7-cv-726-LMB-JFA (E.D. Va. Oct. 12, 2017).

116. Diana Kwon, *Judge Recommends Ruling to Block Internet Access to Sci-Hub*, SCIENTIST (Oct. 4, 2017), https://www.the-scientist.com/daily-news/judge-recommends-ruling-to-block-internet-access-to-sci-hub-30793 [https://perma.cc/S5QR-5BYM].

117. *See* Stoltz, *supra* note 105.

118. According to FED. R. CIV. P. 65(d)(2), "The order binds only the following who receive actual notice of it by personal service or otherwise: . . . (c) other persons who are in active concert or participation with anyone described in Rule 65(d)(2)(A) or (B)." *See* CCIA Amicus Brief, *supra* note 113, at 1.

119. *Id.* at 2.

120. *Id.* at 4. Courts have long interpreted this rule narrowly, explaining that "the only occasion when a person not a party may be punished, is when he has helped to bring about, not merely what the decree has forbidden, because it may have gone too far, but what it has power to forbid, an act of a party." Alemite Mfg. Corp. v. Staff, 42 F.2d 832, 833 (2d Cir. 1930); New York v. Operation Rescue Nat'l, 80 F.3d 64, 70 (2d Cir. 1996); Haizlip v. Alston, No. 1:14CV770, 2015 WL 8668230, at *1 (M.D.N.C. Dec. 11, 2015). In other words, an

However, the uncertainty surrounding this order is not just about to *whom* it applies. *How* this order will be effectively implemented (insofar as the ACS specifically enforces it) and *what* its actual impact on ACS's intellectual property and the public interest in access to knowledge is, also remain unknown.[121] As demonstrated henceforth, different digital measures could be applied to disable access to allegedly infringing websites. These means vary substantially in their costs of implementation, accuracy, and efficiency (potency against circumvention). However, these differences between the varied blocking measures effectively define the scope and breadth of blocking: the more accurate and potent the blocking is, the narrower is the remedy, and vice versa. Of course, the scope and breadth of the remedy, which stem from the specific blocking measure applied, further define the ultimate balancing between the competing rights and interests. These are the rights-holders' intellectual property rights, on the one hand, and third parties' free speech and access to information, on the other.[122] The following discussion briefly explains the differences between major blocking techniques to elaborate this point.

C. VARIED BLOCKING MEASURES

Access to websites may be blocked by various technological means that differ in their technical and policy limitations, as well as in their consequences. In March 2017, the Internet Society—an international organization whose vision is "to promote the development of the Internet as a global technical infrastructure,"[123] published an overview of internet content blocking, which relies on public policy considerations.[124] The overview offers "a technical assessment of the benefits and drawbacks of the most common blocking techniques used to prevent access to content deemed illegal," in order "to help readers understand what each technique can, and cannot, block, along with the

injunction may not "make punishable the conduct of persons who act independently and whose rights have not been adjudged according to law." Regal Knitwear Co. v. NLRB, 324 U.S. 9, 13 (1945).

121. Andrew Silver, *Sci-Hub Domains Inactive Following Court Order: 'Free science'/Pirate Site Operator 'working on solving DNS issue'*, REGISTER (Nov. 23, 2017), https://www.theregister.co.uk/2017/11/23/sci_hubs_become_inactive_following_court_order/ [https://perma.cc/L7FB-LPXT].

122. *See infra* Part IV.

123. *Our Mission*, INTERNET SOC'Y, https://www.internetsociety.org/mission/ [https://perma.cc/5DTR-4ZBN] (last visited Jan. 4, 2020).

124. *Internet Society Perspectives on Internet Content Blocking: An Overview*, INTERNET SOC'Y (Mar. 24, 2017), https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf [https://perma.cc/Z78P-YQ8K] (explaining that there are other motivations for blocking content, such as preventing or responding to network security threats or managing network usage) [hereinafter INTERNET SOC'Y].

side effects, pitfalls, trade-offs, and associated costs."[125] According to this overview (and other similar reports[126]), approximately five main content-blocking methods exist that target the elements of a typical end-user sequence of searching, retrieving, and viewing content with a web browser or similar tool. Note that while these methods may be applied at different points of access—national,[127] individual telecommunication carriers,[128] local network,[129] or endpoint[130]—blockings based on public policy, such as blocking of pirate websites, occur on the national or carrier level.

1. IP Blocking

The simplest website blocking method is based on IP addresses, and its essential goal is to block all traffic to the IP address associated with the designated website. This means that any attempt to connect to a server with that IP address will be interrupted.

In terms of accuracy, this blocking method ranks poorly. To the extent that legitimate content shares the same IP address with the illegitimate content, legitimate content will be inevitably blocked too.[131] In legal terms, this equates to over-enforcement of copyrights, which tilts the balance between free speech and copyright protection to the benefit of the latter. Moreover, the fact that only the hosting provider knows exactly how many websites share the same IP address suggests that IP-based blocking could be quite arbitrary.[132]

Furthermore, the efficiency of this blocking method is also doubtful. IP-based blocking is implemented by devices located between the end-user and the pirate website.[133] Hence, users who are not "behind" the blocking device, because they use the services of an internet provider that has not inserted a

125. *Id.* at 5.

126. *See "Site Blocking" to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act*, OFCOM 26 (May 27, 2010), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78095/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf [https://perma.cc/7PHT-4G7M] [hereinafter OFCOM, *"Site Blocking" to Reduce Online Copyright Infringement*).

127. When all traffic entering or leaving a country may be subject to content blocking.

128. When mobile carriers and traditional ISPs install content blocking tools.

129. When local networks, such as home or school networks, install blocking tools, usually for the purpose of network management or security policy.

130. When software is installed directly on end-user computers, usually for security reasons but also for network management or parental control reasons.

131. INTERNET SOC'Y, *supra* note 124, at 12 (providing a diagram showing how IP blockings could easily result in over-enforcement).

132. Lukas Feiler, *Website Blocking Injunctions under EU and U.S. Copyright Law—Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?* 9–10 (TTLF Working Paper, No. 13, 2012).

133. INTERNET SOC'Y, *supra* note 124, at 13.

blocking device, as well as users who use technology that conceals the true destination of their traffic (such as VPN), can bypass the blocking.[134] Additionally, the effectiveness of IP-based blocking diminishes when website owners use content delivery networks (CDNs) that constantly change the infringing content's IP addresses.[135]

2. Blocking Based on Deep Packet Inspection

Another website-blocking method is based on Deep Packet Inspection (DPI). Unlike IP-based blocking, with deep packet inspect, sophisticated software filters all content according to specific blocking rules.[136]

This method also raises a number of issues. Privacy is particularly threatened because all users' actions that are not encrypted are being inspected.[137] Meanwhile, there are several questions regarding the effectiveness of this blocking method since it cannot inspect encrypted content, even though more than half of internet traffic is encrypted.[138] In terms of costs, this blocking method is considered quite expensive to apply because it depends on the development of filtering software. Since its success rests on the software's ability to identify particular content (according to keywords, traffic characteristics, or filenames), it is more efficient for network management and security enforcement, but not for policy-based blocking, which is far more flexible.[139]

3. URL-Based Blocking

A third website-blocking method is based on the URL. This blocking device may be located on the end-user's computer or in a network between

134. *Id.*
135. *Id.*
136. *Id.* at 14.
137. *See infra* Part IV.
138. Cam Cullen, *The Global Internet Phenomena Report*, SANDVINE (Oct. 2018), https://www.sandvine.com/hubfs/downloads/phenomena/2018-phenomena-report.pdf [https://perma.cc/RW8W-D65M].
139. For instance, some uses of copyrighted material constitute fair use for various policy reasons, such as promoting criticism, enabling research, and supporting education. Yet, fair use is a flexible standard, whose application depends on the specific circumstances of the particular use: (1) the purpose and character of the use; (2) the nature of the copyrighted work; (3) the amount taken; (4) the effect of the use on the market for the copyrighted work. While designing a software that would meet this standard now seems more possible than ever, given the recent developments in big data and machine learning, it is definitely much more complicated than designing a software that meets more rigid black line security rules. *See* Niva Elkin-Koren, *Fair Use by Design*, 64 UCLA L. REV. 1082 (2017). For a skeptical view on this issue, see Dan Burk, *Algorithmic Fair Use*, 86 U. CHI. L. REV. 283, (2019).

the end-user and the rest of the internet.[140] URL is the global address of documents and resources on the World Wide Web; therefore, URL-based blocking is not suitable for blocking non-web applications (such as Voice over Internet Protocol).[141] URL-based blocking can be implemented by proxies, as well as by firewalls and routers that block the connection to the web server requested by the end-user (as indicated by the Hypertext Transfer Protocol request), or otherwise direct web traffic to a different webpage. The blocking device intercepts the flow of web traffic and filters URLs that appear in the blocking list.

This, too, raises concerns. Based on the infrastructure, this method depends on the blocking party's questionable ability to control traffic between the end-user and the internet. Designing such a filter can be quite costly.[142] In terms of accuracy, URL-based blocking may suffer from false positives and false negatives alike. On one hand, it may block legitimate content that resides on a blocked web page (take the Wikipedia model, for instance, where blocking a single web page could block access to additional hyperlinks that are embedded in that page and that may link to legitimate content). On the other hand, content providers can quite easily evade the blocking by changing their file's name or using a different server.[143] Additionally, URL-based blocking monitors web traffic while intervening with users' privacy.[144]

4. Platform Filtering

The fourth blocking method depends on platform filtering implemented by major online services such as search engines, social media platforms, or mobile application stores (such as Apple's App Store or the Google Play store). This blocking method depends on cooperation on the part of platforms that filter out objectionable content, either due to local regulation and government requirements or to the platforms' own terms of service (regarding pornography, for instance).

This method results in inconsistency and ineffectiveness. With regards to inconsistency, users of different search engines, as well as users accessing the internet from different countries (for instance, using the U.S. as opposed to the German version of Google) may be able to retrieve different content.[145] Furthermore, since this blocking method only filters out pointers to illegitimate content, but not actual content—which remains available online

140. INTERNET SOC'Y, *supra* note 124, at 15.
141. *Id.*
142. *Id.* at 16.
143. *Id.*
144. *Id.* at 17.
145. *Id.* at 18.

and accessible through other means of retrieving content—it is considered extremely ineffective.[146]

However, it is still very popular both at the national level, especially in online copyright enforcement,[147] and on a private individual level, because it enforces the right to be forgotten.[148]

5. DNS-Based Blocking

A fifth website blocking method is based on Domain Name Systems (DNS). DNS is an easy, user-friendly system for looking up and retrieving content. Users enter their queries in words, separated by dots (for instance, www.haifa.ac.il), or otherwise enter a specific URL (for instance, https://www.haifa.ac.il/index.php/he/), and the domain name lookup result directs them to the matching IP address (for instance, 132.74.189.243).

The major advantage of DNS-based content blocking over other blocking methods is that it does not rely on designing a complicated filter which intercepts all web traffic—hence it is both privacy-friendly and less expensive to implement.[149] With DNS-based blocking, the DNS resolver validates specific search names against a list of illegitimate names, and whenever there is a match the DNS resolver returns incorrect information, or else declares that the name does not exist, so users' access to content using certain domain names is disabled. To be effective, DNS-based blocking depends on the blocking party having complete control over the end-user's network connection, since both users and content providers can easily avoid this blocking technique by using different internet connections or using an alternative set of DNS servers.[150] Like IP-based blocking, DNS-based blocking may also result in blocking legitimate content which resides in the same server

146. *Id.*

147. *See Government Requests to Remove Content*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/government-removals/overview?removal_requests=group_by:totals;period:&lu=removal_requests [https://perma.cc/95L3-DBFZ] (last visited Jan. 4, 2020).

148. Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), 2014 EUR-Lex CELEX LEXIS 62012CJ0131 (May 13, 2014) (acknowledging users' right to request search engines to remove links to personal data unless a strong public interest suggests otherwise). Google has received more than 3.4 million requests to remove URLs. *See* GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/eu-privacy/overview [https://perma.cc/RLB3-KUGX] (last visited Nov. 16, 2019).

149. INTERNET SOC'Y, *supra* note 124, at 19.

150. *See* Chris Hoffman, *5 Ways to Bypass Internet Censorship and Filtering*, HOW-TO GEEK (Aug. 2, 2016), https://www.howtogeek.com/167418/5-ways-to-bypass-internet-censorship-and-filtering/ [https://perma.cc/7YWU-BX52].

using the same domain name (for instance, management.Haifa.ac.il).[151] Indeed, DNS blocking usually targets the uppermost level of the infringing domain.[152] However, compared to IP-based blocking it is slightly more accurate because it is easier regularly to update lists of domain names. However, it is less effective than IP-based blocking because bypassing DNS-based blocking is even easier than bypassing IP-based blocking.[153]

To summarize, injunctions directing third parties to block users' access to pirate websites could be achieved through various content-blocking means, which diverge in terms of accuracy, effectiveness, and cost. Common to all blocking methods are their robust collateral effects,[154] which impact human rights and shape the balance between clashing rights and interests.[155] Specifically, the particular technical details which underline a specific blocking ultimately define the scope and breadth of the blocking remedy itself: how substantially it will burden the financial interests of the ISP; to what extent it could harm legitimate content; and whether it is expected to work efficiently in preventing piracy.

The example of blocking injunctions is imperative for expressing how central the details of digital remedies' implementations could turn out to be. As explained in the following Part, the significant meaning of the remedy's technical implementation details raises a serious compatibility question, which challenges the ability of the court to fulfill its longstanding duty to exercise its adjudication power in accordance with the rule of law, to competently prescribe remedies that are expected to redress the violation of rights, and to assure these remedies are enforced properly. Since the implementation details of digital remedies are defined and executed outside the courthouse, on private grounds, and considering their ample meaning, the fact that they could surpass the court's dominion calls for special attention.

---

151. INTERNET SOC'Y, *supra* note 124, at 19.

152. OFCOM, *"Site Blocking" to Reduce Online Copyright Infringement*, *supra* note 126, at 34. In the domain hierarchy, the top-level domains are represented by extensions such as ".com," ".eu," ".edu," etc.

153. *Id.*

154. *Id.*; Geiger & Izyumenko, *supra* note 85, at 11–16.

155. *See infra* Part IV.

IV. DIGITAL REMEDIES, JUDICIAL DECISION MAKING AND THE RULE OF LAW

Most, if not all, remedy law scholars would agree that "the available remedy influences the content of the right that courts articulate in a given case."[156] This close remedy-right interdependence suggests that prescribing remedies is a fundamental stage in judicial decision making.[157] Specifically, in relation to equitable remedies, courts enjoy relatively broad discretion to fashion remedies that are appropriate to the justice of the particular case.[158]

But this discretion is limited.[159] Like any other exercise of judicial decision making, when judges apply their remedial power, they must preserve the rule of law and exercise their discretion competently, fairly, and transparently.[160] Generally, the rule of law has long been interpreted as comprising two basic ideas: first, that individuals should be governed by law rather than by the arbitrary will of others;[161] and second, that no person is above the law.[162] The law must be clear, so people can develop reliable expectations and make autonomous choices accordingly. Judges are hence "expected to give a reasoned explanation of the process by which they reach their conclusions."[163] In application to the prescription of judicial remedies, it is fair to posit that courts are expected to delineate a clear and precise redress, which expresses a delicate balance between the various rights and interests of those who might

156. Leong, *Making Rights*, *supra* note 10, at 416; Kermit Roosevelt III, *Aspiration and Under Enforcement*, 119 HARV. L. REV. F. 193, 194 (2006) (arguing that remedial considerations exert an important influence over the shape of the standards courts adopt to implement constitutional rights).

157. *See, e.g.*, Mitchell N. Berman, *Constitutional Decision Rules*, 90 VA. L. REV. 1, 43–50 (2004); Laurin, *Rights Translation*, *supra* note 10, at 1007–08.

158. Doug Rendleman, *The Triumph of Equity Revisited: The Stages of Equitable Discretion*, 15 NEV. L.J. 1397, 1402–03 (2015) (providing two examples of equitable discretion in equity areas: one in family law and one in property law).

159. *See* Heine v. Levee Comm'rs, 86 U.S. 655, 658 (1873) (rejecting the notion that a court of equity may "depart from all precedent and assume an unregulated power of administering abstract justice at the expense of well-settled principles"); PHILIP HAMBURGER, LAW AND THE JUDICIAL DUTY 142–43 (2008) (describing "equitable discretion" in the eighteenth century as "a discernment of circumstances" sometimes "beyond reconsideration on error, but this was not to say it was necessarily beyond rules of either equity or law").

160. Guri Ademi, Comment, *Legal Intimations: Michael Oakeshott and the Rule of Law*, 1993 WIS. L. REV. 839, 845 (1993).

161. ALBERT V. DICEY, INTRODUCTION TO THE STUDY OF THE LAW OF THE CONSTITUTION 189–90 (10th ed. 1959).

162. *Id.* at 193.

163. Maria L. Marcus, *Judicial Overload: The Reasons and the Remedies*, 28 BUFF. L. REV. 111, 114 (1979).

be affected from the remedy granted. In short, we expect judges to dominate the scope and reach of the remedies they grant.

Some remedies, however, make it difficult for judges to exercise complete control over the remedies they grant and anticipate their ultimate impact. As explained earlier, "remedies compelling either action or inaction," for instance, often present a problem of "specifying, measuring, and ensuring compliance."[164] In particular, equitable remedies "are costly to administer because they do more than transfer a lump sum from defendant to plaintiff, the standard 'legal' remedy."[165] Digital remedies, as a sub-category of equitable reliefs, take these concerns to the next level. Not only are there substantial underlying digital details determined outside the courthouse, these details are very hard to appreciate and control.

First, digital remedies have a robust impact on the rights and interests of numerous stakeholders. Second, the implementation details of digital remedies are dynamic in their implications, costs, and capabilities of adjusting to the changing digital landscape. And third, the implementation details are embedded in privately-developed, non-transparent codes. The following discussion describes these unique attributes of the means used to implement digital remedies and explains how they challenge the ability of courts to engage in responsible decision making.

A. ROBUST IMPACT ON NUMEROUS STAKEHOLDERS

Digital reliefs are directed to cyberspace and, therefore, they are inherently widespread in their impact.[166] Whether sought to interfere with the operation of digital devices, such as a streaming device (e.g., TickBox[167]) or a smartphone (e.g., iPhone[168]), or otherwise to manage online content (e.g., block online copyright infringement[169]), digital reliefs have a robust effect on numerous actors, far exceeding their direct impact on the parties to the legal dispute. Even when it appears that courts narrowly tailor digital reliefs—for instance, when courts order to disable access to specific websites or to decrypt a particular iPhone—digital reliefs unfold in a wide-reaching fashion.

In particular, the implementation of digital remedies could have a substantial impact over the fundamental rights of numerous internet users who are not direct parties to the legal dispute and, thus, whose interests are not

164. Bray, *supra* note 21, at 563.
165. Avitia v. Metro. Club of Chi., Inc., 49 F.3d 1219, 1231 (7th Cir. 1995).
166. Mulligan & Bamberger, *Saving Governance by Design*, *supra* note 17, at 739.
167. *See supra* note 69 and accompanying text.
168. *See supra* note 72 and accompanying text.
169. *See supra* note 116 and accompanying text.

necessarily adequately represented. For instance, blocking users' access to legitimate online content could curtail their First Amendment rights to freely consume information in the marketplace of ideas.[170] When the operators of TickBox issued a software update to delete all infringing applications from their devices to comply with the court's digital injunction, they essentially diminished their users' ability to consume non-infringing content through these apps or otherwise make non-infringing uses of the content, while also limiting their users' freedom of expression. The same is true in relation to the implementation of website-blocking injunctions, which obviously limit users' right to receive information.[171]

Besides the right to freedom of expression, the implementation of digital remedies may also affect users' privacy. The order which compelled Apple to develop a technological "backdoor" to allow law enforcement agents to break into the locked iPhone of the deceased shooter in San Bernardino is a prominent example.[172] If Apple had complied with the order and written a code to unlock its strong security system, it would have put the data of millions of individuals, inside and outside the United States, at serious risk of unwarranted surveillance, potentially making them victims of crime.[173] Moreover, had the FBI won this legal battle, other technology companies might have followed suit, redesigning their security features to accommodate what they might have interpreted as a judge-made requirement: to design technological backdoors to their digital devices.[174] The order could have had a worrying impact on both national and international security, particularly

> whether used by a black hat hacker who might infiltrate Apple systems, a future FBI investigation emboldened by [the court's] order to apply the precedent in other less compelling settings, or a dictatorship looking for new ways to oppress people that might cite

170. *See* Jerome A. Barron, *Access to the Press—A New First Amendment Right*, 80 HARV. L. REV. 1641, 1666–78 (1967); Jamie Kennedy, Comment, *The Right to Receive Information: The Current State of the Doctrine and the Best Application for the Future*, 35 SETON HALL L. REV. 789, 789–90 (2005); Susan Nevelow Mart, *The Right to Receive Information*, 95 LAW LIBR. J. 175, 175 (2003).

171. *See* Geiger & Izyumenko, *supra* note 85, at 49.

172. *See* Mulligan & Bamberger, *Saving Governance by Design*, *supra* note 17, at 722–26.

173. *See* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 4, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, (No. CM 16-10 (SP)) (C.D. Cal. Feb. 25, 2016).

174. *See* Mulligan & Bamberger, *Saving Governance by Design*, *supra* note 17, at 726.

> the company's compliance with this FBI demand as a reason to comply with those of its own intelligence agencies.[175]

Indeed, while the FBI framed its demand as addressing a single phone, in practice, the implementation of the order would necessarily place the security of millions of other devices and the people who use them at risk.[176]

Similarly, the implementation of the TickBox injunction discussed earlier could also affect the privacy of numerous end users. As the court noted, deleting applications that are independently downloaded by users because they induce copyright infringement may require TickBox operators to hack into their users' devices.[177]

An additional circle of stakeholders which might be significantly affected by the grant of some digital reliefs are those acting "in concert or active participation" with the defendants, who might be compelled to abide by the court injunction even though they are not party to the action brought by plaintiffs.[178] The *Sci-Hub* injunction, for instance, required that

> any person or entity in privity with Sci-Hub and with notice of the injunction, including any Internet search engines, web hosting and Internet service providers, domain name registrars, and domain name registries, cease facilitating access to any or all domain names and websites through which Sci-Hub engages in unlawful access to, use, reproduction, and distribution of ACS's trademarks or copyrighted works.[179]

Holding such a broad spectrum of actors accountable for pursuing the open-ended outcome of restricting access to particular websites may exceed the boundaries of Rule 65 of the Federal Rules of Civil Procedure.[180] However, this debate is beyond the scope of this paper.

Yet, even assuming that such an injunction is procedurally permitted, requiring distinct intermediaries to actively cooperate in its implementation may affect both their free speech and business interests. First, it interferes with distinct online intermediaries in setting and employing "their own content

---

175. Shahid Buttar, *Apple, Americans, and Security vs. FBI*, ELECTRONIC FRONTIER FOUND. (Feb. 20, 2016), https://www.eff.org/deeplinks/2016/02/apple-americans-and-security-vs-fbi [https://perma.cc/94B8-HTSW].

176. *Id.*

177. *See* CCIA Amicus Brief, *supra* note 113.

178. *See* Husovec, *supra* note 93, at 12.

179. Magistrate Judge's Proposed Findings, *supra* note 104, at 12.

180. *See* FED. R. CIV. P. 65(d)(2)(C).

standards."[181] Second, it inflicts high compliance costs on nonparties[182] without affording them the opportunity to object, raising serious due process concerns.[183] To satisfy procedural due process, sufficient evidence showing that remote intermediaries have aided and abetted the defendants in circumventing the injunction issued, or are likely to do so, should be presented in a proceeding where those entities are given an opportunity to be heard.[184] Nonetheless, at least in the *Sci-Hub* case, none of these entities had their day in court. Hence their interests remained largely unrepresented.[185]

Moreover, as demonstrated in Part III above, blocking injunctions, for instance, could affect providers of legitimate content that might be unintentionally blocked due to over-enforcement.[186] This depends on the accuracy of the blocking method applied: the less accurate the method is, the more likely it is to block non-infringing content, as well. Such restrictions of legitimate speech would potentially harm the rights and interests of content providers. Regarding the *TickBox* injunction, for example, software deleted in response to the court's injunction may include applications that link to legitimate content, such as CBS, WatchESPN, The Weather Channel, or Cartoon Network.[187] This means that in addition to impairing the rights of users to access non-infringing content, the implementation of the injunction could also violate the rights and interests of various speakers.

These examples suggest that the overall impact of digital remedies could far exceed the particular rights and interests of the direct parties to the legal dispute. Fair and appropriate prescription of digital remedies requires a thorough consideration of the fundamental rights held by numerous stakeholders, which must be balanced against other important interests such as public safety and security, access to information, or various business

---

181. Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1002 (2008).

182. *See, e.g.*, Case C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 2011 E.C.R. I-12006; Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, 2012 EUR-Lex CELEX LEXIS 62010CJ0360 (refusing to grant a website-blocking order, reasoning that its high implementation costs as well as its complexity would overburden the service provider).

183. *See, e.g.*, Feiler, *supra* note 132.

184. *See* Mullane v. Cent. Hanover Bank & Tr. Co., 339 U.S. 306, 313 (1950).

185. *See* Magistrate Judge's Proposed Findings, *supra* note 104, at 4.

186. *See supra* notes 131–155 and accompanying text.

187. Response in Opposition to Motion for Preliminary Injunction at 3, Universal City Studios v. TickBox TV, No. 17-7496 (C.D. Cal. Dec. 28, 2017).

interests,[188] especially given that these rights and interests are not necessarily voiced during the regular legal process.[189] The problem, however, is that it is not enough to make this consideration in advance because translating legal balances into digital processes may result in alterations of meaning.[190] Indeed, digital remedies are open to different implementations, and these are subsequently interpreted and embedded in proprietary codes.[191]

Alteration of meaning may occur twice: First, when the private operator who executes the order decides which digital measure to apply in order to achieve the desired outcome. Second, when program developers create the code which applies this measure. Thus, even if digital remedies could reflect a broad and inclusive deliberation of diverse rights and interests, their practical, out-of-court implementation could effectively reshape settled legal balances. But if courts cannot anticipate how digital reliefs unfold, they cannot ensure that they are actually fit to redress specific violations of rights, and this further challenges the rule of law.

Consider, for instance, the implementation of content-blocking injunctions. Normally, under settled copyright doctrine, content is allowed unless it is found to be infringing,[192] creating a delicate balance between the property rights of current creators and the freedom of expression of future ones.[193] Nevertheless, as shown in Part III, content-blocking techniques may over-enforce copyrights and block legitimate content, at the expense of the rights of creators of legitimate content and the public at large. Similarly, if the FBI had not withdrawn its motion to compel Apple to develop a technological

188. Geiger & Izyumenko, *supra* note 85, at 77–82 (discussing the economic impact of copyright website blockings on ISPs, which are not only complex but also quite expensive to implement).

189. *Ex parte* demands, such as the FBI's demand in the Apple v. FBI dispute, normally completely deprive the court of defendant's perspective altogether. Bamberger & Mulligan, *Saving Governance by Design*, *supra* note 17, at 723. In the Apple v. FBI dispute, however, Apple and numerous organizations did receive an opportunity to raise their concerns because the FBI filed a motion to compel Apple to comply with the assistance order. *Id.*

190. *See* Austl. Admin. Rev. Council, *Automated Assistance in Administrative Decision Making*, Issues Paper No. 35, 18–19 (2003), https://www.ag.gov.au/LegalSystem/AdministrativeLaw/Documents/practice-guides-and-other-publications/automated-assistance.pdf [https://perma.cc/GQK4-JPTL]; James Grimmelmann, *Regulation by Software*, 114 YALE L.J. 1719, 1727–28 (2005).

191. *See infra* Section IV.C.

192. Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 683 (2006).

193. As stated by James Madison, the framer of the Constitution's Copyright Clause, "the public good fully coincides . . . with the claims of individuals." *See* THE FEDERALIST NO. 43 (James Madison).

backdoor to its iPhone security system, and other technology companies had followed suit, adjusting their devices' security features so as to make them breakable, the balancing of rights and interests initially set by the court could have been skewed. Even if, originally, surveillance was to be allowed only in this particular case to protect public security, by now accessing personal data without the owner's consent could have become generally easier, while imposing a serious threat to users' privacy.[194]

To sum up, the ways in which digital remedies unfold have a widespread affect over innumerable right holders. Even if judges could potentially afford adequate consideration to all the rights and interests on the table, the problem remains unresolved: the out-of-court, digital implementation of digital remedies could practically redefine judicial balances and have dramatic impacts on settled law.

B. DYNAMIC AND ONGOING IMPACT

Another major problem with digital remedies which further complicates courts' capacity to control and anticipate how they evolve relates to the dynamic nature which surrounds their implementation. Unlike judicial reliefs that provide a "one-shot" solution to a legal dispute, any application of structured technological solutions to resolve legal disputes arising in the digital ecosystem must be able to adjust to a rapidly changing technological environment.[195] For instance, blocking access to pirate websites could be easily circumvented if users and content providers conceal their online conduct by using VPNs, proxy services, and the like.[196] History has taught us that the circumvention of digital locks is only a matter of time and persistence.[197] This suggests that the efficacy of content blocking is, at most, temporary. But if their effectiveness decreases, what is left to compensate for the censorship of legitimate content? To address this issue, digital remedies must allow for timely adaptations.

Moreover, digital remedies are often directed to resolving an ongoing problem, which further blurs their anticipated limits. The *Sci-Hub* injunction, for instance, was amended soon after it was initially signed by the court according to a magistrate judge's proposed findings in order to expand ACS's

194. *See* Mulligan & Bamberger, *Saving Governance by Design*, *supra* note 17, at 726.

195. *See id.* at 739.

196. *Supra* Section III.C.

197. The circumvention of Digital Rights Management systems (DRMs) which are supposed to restrict users' use of and access to copyrighted protected works is one example. *See* Brandon Widder, *DRM Getting You Down? Here's How to Strip Your Music and Movies of Restrictions*, DIGITAL TRENDS (Feb. 22, 2015), https://www.digitaltrends.com/home-theater/how-to-remove-drm-from-music-and-movie-files/ [https://perma.cc/TS4G-SWV5].

ability to act against newly registered domain names as well as the domain names already registered when the initial injunction was issued.[198] Without this amendment, ACS would have been "forced to engage in a game of whac-a-mole whereby new sci-hub domain names emerge" rapidly.[199]

Furthermore, unexpected dynamics in the technological environment which surround the implementation of digital remedies could also affect innovation in different and unpredicted ways. The German "free Wi-Fi" experience is an excellent example. In 2010, the German Supreme Court held that a private operator of an open Wi-Fi network should help rights-holders enforce their rights by sufficiently password-locking the network's connectivity in order to prevent possible misuse.[200] Consequently, password-protected Wi-Fi connections became the *de facto* standard in Germany.[201] When subsequent technological solutions became dependent on open Wi-Fi, Germany suffered a serious innovative setback.[202] Hence, the court's failure to anticipate the full impact of the digital remedy it had granted eventually slowed down progress and innovation.

But it is not only the technological environment which surrounds the implementation of digital remedies that is dynamic—it is also the means of implementation themselves, and their potential costs. Consider, for instance, blocking injunctions. European courts have acknowledged that the cost of implementing blocking measures might be quite substantial.[203] As shown previously, these costs vary with the specific blocking technique implemented.[204] However, since the manner of implementation is determined on private grounds, or outside the courthouse, courts cannot really anticipate what would be the total compliance costs, presenting further challenges their

198. Ernesto, *Publisher Gets Carte Blanche to Seize New Sci-Hub Domains*, TORRENTFREAK (Apr. 10, 2018), https://torrentfreak.com/publisher-gets-carte-blanche-to-seize-new-sci-hub-domains-180410/ [https://perma.cc/J6SF-BVUS].

199. *Id.*

200. Husovec, *supra* note 93, at 4–5.

201. *Id.*

202. *See* Loveday Wright, *Germany's Wi-Fi Problem*, DW (Nov. 13, 2014), https://www.dw.com/en/germanys-wi-fi-problem/a-18060000 [https://perma.cc/6UMZ-NLKS].

203. *See, e.g.*, Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH 2014 EUR-Lex CELEX LEXIS 62012CA0314 (May 19, 2014) Bus LR 541; Case C-70/10, Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM), 2011 E.C.R. I-12006 , ¶ 50; Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, 2012 EUR-Lex CELEX LEXIS 62010CJ0360 (Feb. 16, 2012) (holding that the application of content filtering technology is too expensive and therefore ISPs cannot be obliged to include filtering in their services).

204. *See supra* Section III.C.

ability to exercise their remedial power in a fair and competent manner. How could they grant a relief of which its economic burden is unknown?

Additionally, to the extent that digital remedies are implemented through evolving measures, such as machine learning algorithms, the ability to anticipate their final reach becomes even more complicated. Thanks to recent developments in big data, some digital remedies may rely on advanced capabilities of machine learning to pursue their objectives more efficiently. For instance, different content-blocking methods, especially platform, URL, or DPI-based blocking, depend on filtering technologies that monitor all content that is available in the network.[205] These content filters could be designed to identify trends, relationships, and hidden patterns in disparate sources of content, which are then used to shape users' experience.[206] Yet, while shaping performance based on experience could be particularly valuable for implementing flexible policy-based blocking of copyright-infringing content, it is very hard to follow and predict its potential impact.

C. NON-TRANSPARENT IMPLEMENTATION ON PRIVATE GROUNDS

Real-world compliance with judicial remedies is generally clear-cut and its underlying objectives are self-evident. This is because physical actions (or inactions) are generally easy to check: selling goods, erecting a fence, or avoiding trespassing. The implementation of digital remedies, on the other hand, is often embedded in proprietary black-box codes, which could be very difficult to evaluate.[207] Consider again, for example, the *TickBox* injunction, which essentially compelled TickBox to issue a software update that would delete all software that enabled users to access copyright-infringing content.[208] The practical breadth of this proprietary software update is unknown and largely unknowable.[209] One theory posits that TickBox released a software

205. *Id.*

206. Perel & Elkin-Koren, *Black Box Tinkering*, *supra* note 2, at 189.

207. Rob Kitchin, *Thinking Critically About and Researching Algorithms* 7 (The Programmable City, Working Paper No. 5, 2014), http://ssrn.com/abstract=2515786 [https://perma.cc/UYB9-KHCK]; Perel & Elkin-Koren, *Accountability in Algorithmic Enforcement*, *supra* note 1, at 476; Citron, *Technological Due Process*, *supra* note 1, at 1261–62; Tal Z. Zarsky, *Governmental Data Mining and Its Alternatives*, 116 PA. ST. L. REV. 285, 293 (2011); Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1552 (2013).

208. *See supra* Section III.A.

209. *See, e.g.*, Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 259–60 (S.D.N.Y 2008) (refusing to force YouTube to provide Viacom with the computer source code which controls both YouTube.com's search function and Google's internet search tool "Google.com," explaining that "[t]he search code is the product of over a thousand person-years of work" and "[t]here is no dispute that its secrecy is of enormous commercial value." Earlier cases invoked trade secrets in Google's ranking algorithm); *see also* Kinderstart.com L.L.C. v. Google,

update that removed copyright-infringing addons from previously shipped devices.[210] Since it must block access to "any 'build,' 'theme,' 'app,' 'addon[,]' or other software program that TickBox knows or has reason to know links directly or indirectly to third-party cyberlockers or streaming sites that transmit unauthorized performances of copyrighted motion pictures or television shows,"[211] it might also block access to additional, non-infringing, content. As rigorously contended by TickBox, many software programs designated by the plaintiffs in their complaint had substantial non-infringing uses, allowing users to access legitimate content.[212] Deleting these software programs would thus inevitably result in restricting even lawful content.[213] Hardly apparent, however, is precisely *which* pieces of content would be affected.

The same applies to the technological backdoor feature Apple was requested to design. Again, if Apple had designed a code enabling the FBI to access the terrorist's locked iPhone, it would have probably been impossible to work out how it functioned.[214] To begin with, such a code would have probably been protected under trade secret law.[215] In fact, when the FBI dropped its case against Apple after a private tech firm managed to break into

---

Inc., No. C 06-2057 JF (RS), 2006 WL 3246596, at *1–2 (N.D. Cal. July 13, 2006) (granting Google's motion to dismiss and holding that Google's use of secret methods to compile search results does not amount to anticompetitive conduct); MICHAEL J. MADISON, OPEN SECRETS IN THE LAW AND THEORY OF TRADE SECRECY 222, 241 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011).

210. *See Tickbox Customers: They're About to Remotely Wipe Your Devices Without Your Consent*, TVADDONS (Feb. 14, 2018), https://www.tvaddons.co/tickbox-remote-wipe/ [https://perma.cc/6428-3GVG].

211. TickBox 2, *supra* note 69, at 1.

212. TickBox Response in Opposition to Motion for Preliminary Injunction, Universal City Studios Prods. L.L.L.P. v. TickBox TV L.L.C., No. 2:17-cv-07496-MWF (ASX), at *3 (C.D. Cal. Feb. 13, 2018) ("[T]he Box is simply a small computer which performs common and non-infringing functions of any smartphone, tablet, or desktop computer, and allows its users the ability to download a number of third-party applications that provide users access to authorized streaming content directly from content providers.").

213. *See* Annemarie Bridy, *A New Front in the Set-Top Box Piracy Wars: Can SONY'S Safe Harbor Save TICKBOX TV?*, CTR. INTERNET & SOC'Y STAN. L. SCH. BLOG (Nov. 26, 2017), http://cyberlaw.stanford.edu/blog/2017/11/new-front-set-top-box-piracy-wars-can-sony%E2%80%99s-safe-harbor-save-tickbox-tv [https://perma.cc/9LGW-8L6V].

214. *See* Pasquale, *Restoring Transparency to Automated Authority*, *supra* note 2, at 237 (explaining how "[t]rade secrecy law also makes it all the more important to keep algorithms secret").

215. Perel & Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, *supra* note 1, at 522–23.

the terrorist's phone, the FBI refused to reveal the identity of that third party or to disclose the method it had developed in order to access the iPhone.[216]

Indeed, with digital remedies, choosing between various implementation possibilities and applying them is done on private grounds, outside the courthouse, notwithstanding its important implications for the rule of law, human rights, and innovation. The defendants effectively operate as law makers, only without the safeguards which normally restrain traditional law making. To some extent, they "act as both a judge and an executioner, performing functions of great importance to the public which are normally reserved [for] authorized governmental bodies."[217] Nevertheless, as private actors, defendants are generally free to manage their own business in an undisturbed fashion.[218] While they arguably hold the necessary expertise to develop and implement the proper technology which will fit the digital remedy, they lack the responsibility to take into account broad and inclusive considerations that go beyond the defendants' obvious economic interest. Delegating the power to shape the ultimate scope and reach of digital remedies to private parties, hence, risks privileging their own economic interests.[219] For instance, leaving service providers with broad discretion to elect how to implement a blocking injunction may result in encouraging them to apply the cheapest blocking techniques, regardless of their efficacy or accuracy.

One possible way to address this issue of privatization is to grant technology-specific remedies. Particularly, courts could arguably point at specific digital measures that must be applied in order for the defendant to comply with the injunction. For example, Apple was required to accomplish three functions: (1) bypass or disable the self-destruct function on the phone; (2) allow the FBI to submit passcodes to the phone through electronic testing; and (3) ensure that software running on the phone would not introduce

---

216. Romain Dillet, *Justice Department Drops Lawsuit Against Apple as FBI Has Now Unlocked Farook's iPhone*, TECHCRUNCH (May 29, 2016), https://techcrunch.com/2016/03/28/justice-department-drops-lawsuit-against-apple-over-iphone-unlocking-case/ [https://perma.cc/USF5-D3KA]. Note that a district judge had subsequently approved the FBI's refusal, ruling that it was not required to provide records relating to vendor identity under Exemptions 1, 3, and 7(E) of the Freedom of Information Act. *See* Associated Press v. FBI, 265 F. Supp. 3d 82 (D.C. Cir. 2017).

217. Perel & Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, *supra* note 1, at 485.

218. *See* John Eden, *Why Apple is Right to Resist the FBI*, TECHCRUNCH (Mar. 13, 2016), https://techcrunch.com/2016/03/13/why-apple-is-right-to-resist-the-fbi/ [https://perma.cc/V4PY-STQJ] ("The FBI has no underlying right to compel Apple to create new software products.").

219. Bamberger & Mulligan, *Saving Governance by Design*, *supra* note 17, at 742.

additional delays between passcode attempts.[220] Judge Pym further advised Apple with regards to what it should actually do to reasonably pursue these functions, providing a recommended map of the specific technological actions that should be taken.[221] At the same time, however, since a privately developed code could be a form of protected speech,[222] the judge also allowed Apple to use alternate technological means as long the government concurred and these means achieved the functions designated in the order, as well as the functionality described in the technological map provided by the court.[223]

Technology-specific remedies arguably restrain the private executor's discretion in choosing the technological means to implement the injunction; still, they remain just as vague as open-ended injunctions. Indeed, as it is a private executor who eventually implements the injunction outside the courthouse, it remains difficult to check how far she applies the technological steps that the court has initially set forth. After all, these steps would be later embedded in proprietary technology, which is inherently non-transparent.

Moreover, the allegedly increased predictability of technology-specific injunctions may come at the price of hindering innovation and encumbering the accumulation of new technologies. This is because a particular technological map for achieving a specific legal outcome can only consider known technologies and their known pros and cons. However, technology changes rapidly. New technologies replace old ones, newly discovered attributes of old technologies may improve or negate their capabilities, and new combinations of technologies may expand their individualized effect.

---

220. Order Compelling Apple Inc. to Assist Agents in Search at 8, *In re* Search of an Apple iPhone, No. ED 15-0451M (C.D. Cal. Feb. 16, 2016).

221. *Id.* ¶ 3.

222. Kim Zetter & Brian Barrett, *Apple to FBI: You Can't Force us to Hack the San Bernardino iPhone*, WIRED (Feb. 25, 2016), https://www.wired.com/2016/02/apple-brief-fbi-response-iphone/ [https://perma.cc/J2L8-NT7G] (referencing Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (vacated) which held that "software, in its source code form . . . must be viewed as expressive for First Amendment purposes"); Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 32, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (C.D. Cal. Feb. 25, 2016) ("The government asks this Court to command Apple to write software that will neutralize safety features that Apple has built into the iPhone in response to consumer privacy concerns. . . . This amounts to compelled speech and viewpoint discrimination in violation of the First Amendment."). *But see* Neil Richards, *Apple's "Code=Speech" Mistake*, MIT TECH. REV. (Mar. 1, 2016) (explaining that "[t]he Supreme Court has never accepted that code is protected like speech").

223. Order Compelling Apple Inc. to Assist Agents in Search, No. ED 15-0451M at ¶ 4 (Feb. 16, 2016).

Considering the ongoing nature of digital remedies discussed earlier, the need to adjust them from time to time is clear. However, confining executors' discretion to the technological standards applicable "back then," or when the court first issued its injunction, could hinder the development of better digital solutions going forward. To illustrate, curbing Apple's technological discretion might have forced it to follow the technological map provided by the court, which may not necessarily always be the most appropriate way to gain access to a locked iPhone. Presumably, Apple is in the best position to intervene with its own private technology in the least harmful way, and a technology-specific injunction could encumber that expertise, impeding the development of better, innovative solutions.

Apple, for instance, could have followed the technological map provided by the court in its order, but it could also have used alternative technological means to achieve this outcome while still being in compliance with the order. The government would likely have been satisfied either way, as long as it got access to the specific type of data it presumably sought: data indicating whether the shooter was acting independently or on behalf of a terror organization.[224] But successfully breaking into an iPhone is not the only thing that matters.

Equally as important are the *means* applied to achieve the outcome, especially when these may differ in their capabilities and costs, which in turn may directly impact human rights. GrayKey, for instance, is a small device which law enforcement agents use to access locked iPhones.[225] It takes GrayKey anywhere from an hour or two to a few days to guess an iPhone's password and give its operator full access to the phone's file system, including messages, photos, call logs, browsing history, and passwords.[226] However, an alternative device could be developed that would provide restricted access to data stored on locked iPhones which would be less intrusive to users' privacy. Such a device, for example, could restrict data portability, limiting law

224. Ann Kristin Glenser, *Decrypting Apple: Making Technology Companies the Referees of Law Enforcement on Privacy*, JOLT DIG. (June 7, 2017), https://jolt.law.harvard.edu/digest/decrypting-apple-making-technology-companies-the-referees-of-law-enforcement-on-privacy [https://perma.cc/U5VK-YJFL].

225. Zack Whittaker, *For $15,000, GrayKey Promises to Crack iPhone Passcodes for Police*, ZDNET (Mar. 19, 2018), https://www.zdnet.com/article/graykey-box-promises-to-unlock-iphones-for-police/ [https://perma.cc/SD47-2BHX]. However, Apple had very recently released a new feature, iOS 11.4.1, to address this security loophole. This feature requires users to unlock their device after an hour of inactivity to connect a USB accessory to make it more difficult for police to use GrayKey to unlock iPhones. *See* Isobel Asher Hamilton, *Apple is Reportedly Closing a Security Loophole that will Prevent Police from Accessing iPhones*, BUS. INSIDER (July 14, 2018), http://www.businessinsider.com/apple-will-make-it-harder-for-police-to-access-locked-iphones-2018-6 [https://perma.cc/A4CZ-YS4Z].

226. Whittaker, *supra* note 225.

enforcement agents' ability to transfer the data they access to other devices. While such a hypothetical alternative might be more expensive, and even less effective for law enforcement purposes, it would better preserve privacy.

Overall, the essence of digital remedies is their profound technical details, and these are designed and executed outside the courthouse during implementation. Yet these details are far from being merely procedural; they effectively shape the balance between competing rights and interests held by numerous stakeholders. Given their opaque nature, and considering the dynamic environment in which digital remedies unfold, it becomes rather challenging to appreciate their scope and assure they constitute a fit redress. Therefore, the next and final Part explores how the toolkit of equitable managerial devices and constraints could assist courts in preserving their dominance over digital remedies.

V. OVERSEEING DIGITAL REMEDIES

Overseeing how digital remedies unfold is vital to safeguard the rule of law, to protect human rights, and to ensure they are compatible with the changing digital reality. Although the grant of digital remedies is subject to traditional ex-ante judicial review, this is not enough to ensure courts exercise full and ongoing control of digital remedies. Accordingly, this last Part of the Article recommends several mechanisms that courts could exploit in order to extend their oversight and retain more control over the critical implementation stage of digital remedies. In essence, these tools purport to empower judges who resolve cyber-related disputes with a broader and a more accurate understanding of the meaning of their digital solutions.

This is where the system of equitable remedies comes into play. Recall that previously in Part II, digital reliefs were classified as specific, prospective, and equitable remedies, yet their equitable nature was especially emphasized given that they generally "compel action (or inaction), especially when that action may be continuing or iterative and not easily measured."[227] Stressing the equitable nature of digital remedies is constructive because the system of equitable remedies includes, in addition to the remedy itself, equitable managerial devices that allow courts to manage the parties and ensure compliance, as well as special equitable restraints.[228]

227. Bray, *supra* note 21, at 533.
228. *See id.* at 534.

A. MANAGERIAL DEVICES

Managerial devices generally purport to "enhance the court's ability to manage the parties" and, thus, ascertain compliance.[229] In application to digital remedies, these devices could further enhance the court's overseeing capabilities, allowing them to control the breadth and scope of the reliefs as they evolve. In particular, these devices could mitigate the problem of anticipating what would be the overall impact of particular digital remedies in advance.

1. Ex-Post Revision

The dynamics which surround the implementation of digital remedies, and the rapidly changing ecosystem in which they operate, may warrant ex-post revision. When necessary, courts should exploit their power to revise their remedies in keeping with changing circumstances.[230] The example of the Wi-Fi problem in Germany, mentioned earlier, neatly illustrates the critical need for flexibility.[231] If the German courts had promptly considered adapting their original orders, which compelled private Wi-Fi providers to password-lock their services, when the new Wi-Fi-based technologies began blossoming outside Germany, they might have prevented the innovative setback that Germany suffered as a result of their technological remedies.[232] Indeed, ex-post revision of equitable remedies is tailored to meet the need for flexibility in remedies of injunction or specific performance.[233] This power enables courts to respond to events that were unforeseen when the remedy was first granted, because of changes in law or changes in fact, which typically occur in the digital ecosystem.[234]

---

229. *Id.* at 564.

230. *See id.* at 564–65.

231. *See generally* Mike Masnik, *German Court Says you Must Secure your WiFi or you may Get Fined*, TECHDIRT (May 12, 2012), https://www.techdirt.com/articles/20100512/1116409394.shtml [https://perma.cc/95SU-ZBBS].

232. *See, e.g.*, Loveday Wright, *Germany's Wi-Fi Problem*, Dw (Nov. 13, 2014), https://www.dw.com/en/germanys-wi-fi-problem/a-18060000 [https://perma.cc/6UMZ-NLKS].

233. *See* Bray, *supra* note 21, at 564–65.

234. *See* Salazar v. Buono, 559 U.S. 700, 714–15 (2010) (plurality opinion) ("Because injunctive relief is drafted in light of what the court believes will be the future course of events, . . . a court must never ignore significant changes in the law or circumstances underlying an injunction lest the decree be turned into an instrument of wrong.") (internal emphasis removed); King-Seeley Thermos Co. v. Aladdin Indus., Inc., 418 F.2d 31, 35 (2d Cir. 1969) ("While changes in fact or in law afford the clearest bases for altering an injunction, the power of equity has repeatedly been recognized as extending also to cases where a better appreciation of the facts in light of experience indicates that the decree is not properly adapted to accomplishing its purposes.").

The *Sci-Hub* injunction, for instance, was amended soon after it was first issued, following the plaintiff's request to be given the authority to seize any and all Sci-Hub domain names, including those to be registered in the future.[235] In fact, the ease with which Sci-Hub could close existing domains and open new ones made the original order that targeted specific domains worthless. At the same time, however, content blocking may over-enforce plaintiffs' rights and block legitimate content, while restricting the fundamental rights of third parties that are not direct parties to the dispute and hence do not necessarily have standing to request injunction updates from the court.[236] For this reason, it is critical that courts independently invoke their power to modify remedies whose practical implementation is later found to exceed their original scope.

2. Advising Technical Experts

Furthermore, to subject digital remedies to meaningful oversight, it is vital that courts struggling to resolve cyber-related disputes understand the technological meaning of the relief they consider to grant. In its preliminary ruling in the Motion for Preliminary Injunction filled against TickBox, for instance, the court raised a handful of complex technological questions:

> What is the best way to address the issue of themes (such as Paradox or Lodi Black) and/or addons (such as Covenant) that provide access to unauthorized versions of Plaintiffs' copyrighted work but that Device users have already installed? Is there a way to address this issue? Plaintiffs frame the solution as a simple software update whereby TickBox removes these previously-downloaded themes from its customers' Devices . . . . Is it possible to perform a similar software update whereby all Devices are reset, previously downloaded themes and addons are deleted, and TickBox's customers start anew with an offending-theme-free user interface?[237]

The court, however, did not attempt to answer these critical questions, but rather preferred to maintain the status quo and leave these questions for the parties to address.[238]

But the parties' technological expertise should not negate the need to empower courts with competent and professional capabilities. Out-of-court,

---

235. Ernesto, *Publisher Gets Carte Blanche to Seize New Sci-Hub Domains*, *supra* note 198.

236. Geiger & Izyumenko, *The Role of Human Rights in Copyright Enforcement Online*, *supra* note 85.

237. TickBox 1, *supra* note 68, at 1.

238. *Id.* at 2 ("Keeping these questions and the discussion that follows in mind, counsel for Plaintiffs and TickBox, working with others who possess relevant technical expertise as necessary, shall negotiate and attempt to reach agreement upon a stipulated preliminary injunction that will supersede the Court's initial preliminary injunction order.").

private negotiations about the qualities of a specific relief should not replace responsible decision making, which takes into account the full range of values and interests held by various stakeholders that might be affected by the relief. Specifically, counting on private, out-of-court settlements to reach the most appropriate solution ignores the robustness of digital remedies, the implications of which may far exceed the particular rights and interests of the direct parties to the legal dispute. As demonstrated in Part III, alternative technological solutions may vary in terms of cost, accuracy, and efficiency,[239] and these must be considered and assessed in an unbiased manner. In the United Kingdom, for instance, where blocking injunctions had become a very popular relief against online copyright infringement, Judge Richard Arnold, the undisputed authority when it comes to ordering ISPs to disable access to pirate websites, has been rolling up his sleeves to explore the practical meaning of each blocking alternative and ensure its overall proportionality.[240]

Enhancement of courts' oversight capacity could be achieved by appointing "equitable helpers" with the necessary technical expertise.[241] Particularly, Rule 53 of the Federal Rules of Civil Procedure authorizes judges to appoint special advisors[242] to aid them in handling pretrial matters tried without a jury that cannot be addressed effectively and promptly by available district or magistrate judges.[243] Accordingly, and despite the costs,[244] special masters have been called upon for their expertise in specific fields "such as

---

239. *See supra* Section III.C.

240. *See* Lindsay, *supra* note 88, at 1534–35. For instance, in *Twentieth Century Fox Film Corporation v. British Telecommunication P.L.C.*, Judge Arnold considered:

> [T]he terms of an order requiring [the ISP] to implement [a] hybrid blocking system, concluding that it would be best to frame the injunction as requiring IP address re-routing (to the URL blocking) rather than IP address blocking, as the latter could be disproportionate in that it could result in over blocking [of legitimate speech].

Id. In *Dramatico Entertainment Ltd. v. British Sky Broadcasting*, on the other hand, Judge Arnold held that, "as IP address blocking might prevent circumvention, . . . it could be appropriate for [blocking] to be mandated, provided that the IP address was not shared with non-infringing websites." *Id.* at 1535.

241. *See* Bray, *supra* note 21, at 567–68.

242. *Id.* at 567. There are other authorities for appointing special masters. *See, e.g.*, David I. Levine, *The Authority for the Appointment of Remedial Special Masters in Federal Institutional Reform Litigation: The History Reconsidered*, 17 U.C. DAVIS L. REV. 753 (1984); Wayne D. Brazil, *Authority to Refer Discovery Tasks to Special Masters: Limitations on Existing Sources and the Need for a New Federal Rule*, *in* MANAGING COMPLEX LITIGATION: A PRACTICAL GUIDE TO THE USE OF SPECIAL MASTERS 305 (W. Braz et al. eds., 1983).

243. FED. R. CIV. P. 53(a)(1)(C).

244. *See* Bray, *supra* note 21, at 574.

accounting, finance, science, and technology."[245] Similarly, under Rule 706 of the Federal Rules of Evidence, "trial courts have wide discretion to appoint experts . . . to clarify issues under consideration,"[246] and there is also the "inherent authority [of federal courts] to appoint technical advisors."[247] Hence, if legal disputes which "raise problems of unusual difficulty, sophistication, and complexity, or involve issues well beyond the regular questions of fact and law which judges routinely face" justify the appointment of technical experts and advisors,[248] then complicated and dynamic cyber-related disputes should also warrant such appointment.

3. Imposing Duration Limitations

Constructing equitable remedies in a flexible fashion is considered another equitable managerial device.[249] Specifically, courts could enhance their ability to supervise the implementation of digital remedies by limiting their duration in accordance with their relevance. Because the surrounding digital circumstances change rapidly, as do the technological capabilities to resolve digital problems, courts should regularly consider accompanying digital remedies with proper sunset clauses. Consider, for instance, a blocking order that blocks users' access to a website providing unauthorized live streaming of the NBA finals. Such an order should be limited in time and not exceed the duration of the finals. Otherwise, the risk of over-enforcement and blocking of legitimate content will outweigh the benefit of decreasing copyright infringement.[250]

Limiting the duration of digital remedies will further facilitate their periodic review, which is necessary to allow courts to exploit their ex-post revision power in a timely manner and in light of experience.[251]

---

245. MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.52 (2004). For instance, the appointment of a special master in a case involving intellectual property claims by a manufacturer of medical devices against an inventor and his company who was requested to "mak[e] decisions with regard to search terms; oversee[ ] the design of searches and the scheduling of searches and production; coordinat[e] deliveries between the parties and their vendors; and advis[e] both parties, at either's request, on cost estimates and technical issues." Medtronic Sofamor Danek, Inc. v. Michelson, 229 F.R.D. 550, 559 (W.D. Tenn. 2003).

246. Maayan Filmar, *A Critique of* In Re Bilski, 20 DEPAUL J. ART, TECH. & INTELL. PROP. L. 11, 47 (2009).

247. *Id.* at 48.

248. *Id.*

249. *See* Bray, *supra* note 21, at 568; *supra* note 209.

250. In his blocking injunctions, Judge Arnold, for instance, has "recently imposed a sunset clause, which has time limitation [*sic*] of two years." *See* Husovec, *supra* note 93, at 28.

251. *See* Richemont Int'l SA v. British Sky Broad. Ltd. [2014] EWHC (Ch) 3354, (Eng.) at 373.

For instance, restricting the TickBox injunction to a specified time limit could have enabled the court to promptly find out whether the applications that TickBox effectively deleted were indeed applications that "link[ed] directly . . . to third-party cyberlockers or streaming sites that transmit[ted] unauthorized performances of copyrighted motion pictures or television shows."[252] Indeed, the court had originally raised its concern as to whether prior to deleting any software from TickBox's current user interface, the parties ensured that it actually contained links to the apps or websites that provided access to unauthorized streaming versions of plaintiffs' copyrighted works.[253] Yet, independently reviewing which software was deleted and deciding whether it induced copyright infringement, the court would have to essentially outsource their judicial discretion to private parties' whose judgment might be mistaken or biased. Given the dramatic implications of erroneously restricting free speech, such restrictions should be addressed promptly.

4. Contempt

"Equitable remedies may be enforced by contempt proceedings, through which a court may impose a range of highly discretionary punishments—including a new injunction, the payment of money to the plaintiff, the payment of fines to the state, or, less commonly, imprisonment."[254] While this equitable device is not commonly used, it could nonetheless "allow the court to respond to new circumstances."[255] Effectively, it allows the judge to direct, learn, respond, manage, or substitute for an alternative solution, "all with the goal of achieving the plaintiff's rightful position."[256]

Contempt proceedings could actually have a double effect. From an ex-ante perspective, they require courts to be as clear and precise as possible in defining the remedy,[257] and at the same time, encourage defendants to accurately follow the court's instructions. From an ex-post perspective, like ex-post revision, contempt allows courts to adjust the relief if its practical implementation is found to exceed or override its intended reach. Note that since courts retain the power to review and adjust the remedies they grant,

252. TickBox 2, *supra* note 69, at 1.
253. TickBox 1, *supra* note 68, at 1.
254. Bray, *supra* note 21, at 565–66.
255. *Id.* at 566.
256. *Id.* at 567; *see also* DOUG RENDLEMAN, COMPLEX LITIGATION: INJUNCTIONS, STRUCTURAL REMEDIES, AND CONTEMPT 691–833 (2010).
257. *See* Schmidt v. Lessard, 414 U.S. 473, 476–77 (1974) (per curiam).

detailed architecture of remedies should not diminish their necessary flexibility.[258]

5. Encourage Ongoing Participation of Various Stakeholders

Finally, another mechanism that could facilitate better oversight of the implementation of digital remedies is to give voice to affected users—not only during the initial legal procedure, but also during the subsequent ex-post revision procedures.[259] To avoid lengthy litigation, such participation of interested parties should only be allowed during strict time windows. Since the private, out-of-court implementation of digital remedies may unfold in an unexpected fashion, it is important to allow those whose rights are being affected, as well as those representing various public interests, including non-profits, human rights organizations, law enforcement agencies, and government representatives, to express their concerns before the court and demand the revision of digital remedies that are inefficient or disproportionate (e.g., restricting users' access to legitimate online content). This is especially important in cases where the specific procedural process governing the case negates the possibility of public participation during the early, ex-ante stage of in-court proceedings.

---

258. One example of detailed digital remedy is the blocking order, which was granted in Richemont Int'l SA v. British Sky Broad. Ltd. [2014] EWHC (Ch) 3354, (Eng.), at 319 which reads as follows:

> In respect of its residential fixed line broadband customers [. . .], the [. . .] defendant [ISP] shall within 15 working days in relation to the initial notification (and thereafter, within ten working days of receiving any subsequent notification) adopt the following technical means to block or attempt to block access to the target websites, their domains and sub-domains and any other IP address or URL notified to the . . . defendant whose sole or predominant purpose is to enable or facilitate access to a target website. The technology to be adopted is:
>
> (i) IP blocking in respect of each and every IP address from which each of the target websites operate and which is [. . .] notified in writing to the . . . defendant by the applicants or their agents [. . .]
>
> (ii) IP address re-routing in respect of all IP addresses that provide access to each and every URL available from each of the target websites and their domains and sub-domains and which URL is notified in writing to the . . . defendant by the claimants or their agents; and
>
> (iii) URL blocking in respect of each and every URL available from each of the target websites and their domains and sub-domains and which is notified in writing to the . . . defendant by the [applicants] or their agents.

Id.

259. Mulligan & Bamberger, *Saving Governance by Design*, *supra* note 17, 772–73.

For instance, the FBI's request to the court to force Apple to create software to help them circumvent the phone's encryption was initially submitted as an ex-parte demand.[260] If the FBI had not submitted a subsequent motion to compel Apple to comply with the assistance order,[261] the ex-parte demand would have deprived the court of the perspectives of Apple and numerous organizations that raised diverse concerns about the FBI's request.[262] Similarly, the *Sci-Hub* injunction was ultimately granted as a default judgment, without the defenses of the allegedly direct infringer (i.e., the operator of the Sci-Hub site) or the ultimate enforcers (i.e., various service providers) being heard.[263]

Moreover, encouraging ex-post participation of affected users is especially important for digital injunctions that are directed to non-parties to the legal dispute (e.g., the *Sci-Hub* injunction).[264] Third parties that are required to implement a court order, even though they did not actively represent their interests during the ex-ante judicial procedures,[265] should at least be allowed to deliver their concerns during the stage of ex-post revision considerations. Firstly, because they are not regular non-parties whose interests are affected from the injunction, but are the long hand of the defendants that are effectively expected to obtain the resolution of the case, sometimes even on behalf of the defendants. Secondly, and relatedly, because the economic expenses of executing the remedy could be quite substantial.[266] Thirdly, because when digital remedies delegate adjudication powers to these third parties, directing them not only to choose *which* technological means to apply, but also to decide *how* to implement these means, it is important to provide them with an open

260. Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search at 1–2, *In re* Search of an Apple iPhone, https://epic.org/amicus/crypto/apple/In-re-Apple-FBI-AWA-Application.pdf [https://perma.cc/T2SK-JP74].

261. *See* Government's Motion to Compel Apple Inc., *supra* note 72.

262. *See* Mulligan & Bamberger, *Saving Governance by Design*, *supra* note 17, at 723.

263. *See* Diana Kwon, *American Chemical Society Wins Lawsuit Against Sci-Hub*, SCIENTIST (Nov. 7, 2017), https://www.the-scientist.com/news-opinion/american-chemical-society-wins-lawsuit-against-sci-hub-30648 [https://perma.cc/A8JM-S9D3].

264. *See supra* Section III.B.

265. Generally, many courts apply a four-factored test for issuing preliminary injunctions, which inquire into: (1) whether the plaintiff will suffer irreparable harm absent the issuance of an injunction; (2) how the harm suffered by the plaintiff absent an injunction balances against the harm that an injunction would cause to the defendant; (3) the plaintiff's likelihood of success on the merits; and (4) the public interest. *See* CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 2948, 133 (2d ed. 1995). "Many courts interpret the public interest factor as a license to consider the impact that granting or denying injunctive relief will have on non-parties." Laura W. Stein, *The Court and the Community: Why Non-Party Interests Should Count in Preliminary Injunction Actions*, 16 REV. LITIG. 27, 29 (1997).

266. *See supra* Section III.C.

judicial venue where they can seek technical advice and obtain feedback about their specific compliance. Otherwise, they might be left alone in the battlefield of compliance, which might encourage them to prefer robust technological means with a higher risk of over-enforcement,[267] over specifically tailored reliefs that are more accurate, but might result in under-enforcement.[268]

B. EQUITABLE CONSTRAINTS

The exploitation of the various managerial devices discussed above can be costly, both on the part of the court, especially when nominating technical advisors,[269] and on the part of defendants, especially when required to adjust their compliance in accordance with the changing digital circumstances.[270] Indeed, "equitable remedies have certain characteristic costs, especially the direct and indirect costs of complying with the court's command and the possibility of an afterlife in which that command is clarified, modified, enforced, or dissolved."[271] This is why equitable enforcement tools are subject to various limits.

For instance, there is the doctrine of ripeness, which ensures "the appropriateness of judicial review" in a given case.[272] "Ripeness is especially important for equitable remedies because they can depend on facts that are changing and contingent, and [they] can entangle the courts in the relationship of the parties, not just at the moment of decision but . . . on an ongoing basis."[273] In particular, with regards to digital remedies, it is important to ensure the recourse they provide remains relevant. Additionally, there is the requirement for specificity, "which requires that an equitable decree be precisely worded and give clear notice of what is prohibited and required."[274] Another limit on the use of equitable managerial devices relates to equitable defenses that prevent "the power of these remedies to be used on behalf of a

267. Such as IP blocking. *See supra* Section III.C.

268. Such as the DNS blocking technique of content blocking orders. *See* Feiler, *supra* note 132 and accompanying text.

269. Bray, *supra* note 21, at 573–74.

270. Gene R. Shreve, *Federal Injunctions and the Public Interest*, 51 GEO. WASH. L. REV. 382, 389 (1983) ("[An injunction] poses the threat of adjusting more aspects of the defendant's behavior than those that would wrong the plaintiff if the injunction were not issued. It is difficult if not impossible to so finely adjust an order that it protects plaintiff without impairing defendant's harmless activities or the rights of those who are not represented before the court.").

271. Bray, *supra* note 21, at 577.

272. *See*, *e.g.*, G. Joseph Vining, *Direct Judicial Review and the Doctrine of Ripeness in Administrative Law*, 69 MICH. L. REV. 1443, 1446 (1971).

273. Bray, *supra* note 21, at 579.

274. *Id.*; *see also* FED. R. CIV. P. 65(d).

plaintiff who acts unjustly."[275] For example, plaintiffs cannot bring their claims with unreasonable delay or with unclean hands.[276] Overall, these discretionary limits "focus[] judges' attention on certain situations where equitable remedies and enforcement mechanisms are most likely to be misused."[277]

VI. CONCLUSION

"The devil is in the details," or its predecessor "God is in the details," means that "[t]he details of a plan, while seeming insignificant, may contain hidden problems that threaten its overall feasibility."[278] This phrase captures the precise implication of using technological fixes as solutions for legal disputes: the details underlying such fixes are far from merely procedural. They are actually material, shaping the crux of the technological plan for resolving a concrete legal dispute. Digital remedies change the traditional dichotomy between adjudication and compliance in remedies. They blur the borderline between law making and law enforcement, depositing both powers in the hands of private executors who design and implement the remedy outside the courthouse.

As explained in this Article, digital remedies can be implemented through various means, which differ in their error rate, costs, and circumvention potential. These differences are substantial, as they effectively define the ultimate scope and breadth of the relief. The robust implementation of digital remedies can effectively reshape settled balances between clashing rights and interests and practically dictate progress and innovation.

This critical role of the technical details which underline digital remedies challenges the ability of courts to competently oversee the remedial process. Traditional mechanisms of judicial oversight do not fit the realm of digital remedies. Specifically, ex-ante judicial review, transparent legal procedure, and public participation during legal proceedings ignore all that happens after the court issues its decree, when private, profit-maximizing executors embed their technological choices in non-transparent and proprietary technologies.

An all-embracing perspective of checks and balances is needed to facilitate ongoing, ex-post review of digital compliance, to protect the rule of law,

---

275. Bray, *supra* note 21, at 581.

276. Howard W. Brill, *The Maxims of Equity*, 1993 ARK. L. NOTES 29, 34 (1993) ("The purpose of the unclean hands doctrine is neither to protect the defendant nor to favor the complainant . . . [but] to protect the court . . . .").

277. Bray, *supra* note 21, at 584.

278. *See The Devil is in the Details*, PHRASES FINDER, https://www.phrases.org.uk/meanings/the-devil-is-in-the-details.html [https://perma.cc/HLY7-XKCP] (last visited Jan. 4, 2020).

consider the various rights and interests at stake, and ensure that digital remedies adapt to a rapidly changing digital reality. As suggested in this Article, the exploitation of equitable managerial devices could advance such an all-round perspective, while empowering courts' oversight capabilities. Specifically, by consulting technical experts to hone their technical understanding and implications of the reliefs that will be granted; by supporting ex-post revision of decrees and limiting their duration to address the need for constant adaptation; and by encouraging ongoing participation of various stakeholders to facilitate a broad consideration of human rights and public values, courts could enhance their oversight capabilities while responding properly to the increasing need to resolve cyber-related disputes.