2003

Cybertrespass

Richard A. Epstein

Follow this and additional works at: https://chicagounbound.uchicago.edu/journal_articles

Part of the Law Commons

Recommended Citation

This Article is brought to you for free and open access by the Faculty Scholarship at Chicago Unbound. It has been accepted for inclusion in Journal Articles by an authorized administrator of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.
tion, for while they may not be perfect, at least they have done their job.

B. Application of Traditional Trespass to Chattel to the Internet

The pressure on these rules has mounted with the rise of the internet. Firms and individuals invest substantial amounts of capital and effort to create servers and websites that are linked to the rest of cyberspace via the internet. No technical wizardry is needed to realize that the possibilities for invasions in cyberspace parallel those in physical space. The most obvious illustration of these invasions is spam—those mass messages sent by a single party to all sorts of people who would rather not receive them. It is an open question whether spam counts as a trespass if the spammer has not received any desist message from an internet service provider or ordinary email users (who are not shy to make their concerns known). After all, ordinary phone calls are not trespasses to chattels. But the analysis changes radically once the phone caller or the spammer receives a specific notice asking him to cease and desist. Any implied authorization of the practice is negated by this express command. The rules here are similar to those that govern entering into or remaining on the land of another individual.

But why would one want to stop communications from others? In some cases, the intrusions could be serious enough to overload the computer and perhaps to cause it to crash. In other cases, it might clog the limited capacity of the hard drive or put the owner of the system to some burden to remove the emails in question. On multiple occasions courts have held that these unauthorized intrusions count as deliberate trespasses to chattels, for which either damages or, more critically, injunctive relief should be allowed. It seems impossible to deny

---

14 See, for example, Brad Stone and Jennifer Lin, Spamming the World, Newsweek 42, 43-44 (Aug 19, 2002) (noting Verizon Online’s suit against Al Ralsky, a bulk emailer, for crashing its servers).

15 See, for example, Restatement (Second) of Torts at § 160 (liability for “failure to remove thing placed on land pursuant to license or other privilege”); id § 161 (liability for “[f]ailure to remove thing tortiously placed on land”).

16 See, for example, eBay, Inc v Bidder's Edge, Inc, 100 F Supp 2d 1058, 1060-63 (ND Cal 2000) (granting a preliminary injunction even though Bidder's Edge’s incursions occupied at most only between 1.11 and 1.53 percent of the total load of eBay’s servers); CompuServe, Inc v Cyber Promotions, Inc, 962 F Supp 1015, 1019 (SD Ohio 1997) (granting a preliminary injunction to prevent defendant from continuing to send unsolicited emails to plaintiff’s subscribers). See also Oyster Software, Inc v Forms Processing, Inc, 2001 US Dist LEXIS 22520, *40 (ND Cal) (stating that evidence that defendant made use of plaintiff’s computer is all that is required to sustain a trespass claim); Ticketmaster Corp v Tickets.com, Inc, 2000 US Dist LEXIS 12987, *16-18 (CD Cal), affd, 248 F3d 1173 (9th Cir 2001) (denying injunction because of insufficient proof of trespass and irreparable injury, but noting that the use of a computing system that interferes with regular business is a trespass); America Online, Inc v IMS, 24 F Supp 2d 548, 550 (ED Va 1998) (holding that defendant committed a trespass to chattels by sending unauthorized bulk
that the defendant has entered and used the plaintiff’s facilities, which must in principle count as some form of trespass. The rule on nominal damages is not invoked because harms to equipment, real or threatened, count as actual damages for which both monetary compensation and injunctive relief are appropriate. This new technological innovation offers no reason to bend the traditional rules of chattel trespass to take into account the unique circumstance of the internet.

The key bone of contention, however, arises when defendant’s cyber-entry into the plaintiff’s system causes neither disk damage nor computer slow-down. In these cases, defendants have argued that the nominal damage rule of the Restatement precludes any lawsuits at all. Two cases in which I have written amicus briefs against allowing cybertrespasses, *eBay, Inc v Bidder’s Edge, Inc*17 and *Intel Corp v Hamidi,*18 show the range of arguments that have been used to defeat the claim for injunctive relief in cases of cybertrespass. The two situations were as follows.

*eBay* runs online auctions both great and small. Bidder’s Edge (BE) is (or more accurately was) an auction aggregator whose market niche was to ease the costs of surfing the internet. It did so by consolidating information about the goods and prices available on multiple auction sites. Initially BE sought a license from eBay to gather this information. Similar licenses had been issued to other internet firms such as Yahoo!. These licenses regulated the terms and conditions of access, and also provided the aggregator with small compensation for any business directed to the auction site. But when negotiations between eBay and BE broke down, BE sent its spiders (in other words, probes to find information on the eBay site) on thousands of separate occasions onto the eBay site to gather large amounts of information that BE then displayed on its own site. The theoretical question is: If one brackets any damage to eBay’s equipment or capacity, is this entrance one that eBay is entitled to enjoin? The district court held the unauthorized entry counted as a trespass to chattels which, in light of its repetitive nature, justified injunctive relief.19

In *Hamidi,* the defendant was a former employee of Intel who surreptitiously obtained Intel’s email registry and used it to send inflammatory emails to between eight thousand and thirty-five thousand Intel employees on six specific occasions. Intel claimed loss of productivity attributed to distracted and distraught employees and to

---

17 100 F Supp 2d 1058 (ND Cal 2000).
18 114 Cal Rptr 2d 244, 246 (App 2001) (upholding injunction enjoining a disgruntled former employee of plaintiff from sending thousands of inflammatory emails to other employees), petition for review granted, 118 Cal Rptr 2d 546 (2002).
19 *eBay*, 100 F Supp 2d at 1069–70.
its extended but unsuccessful attempts to keep Hamidi from cracking the website. When Hamidi refused to stop his emails on Intel's request, Intel then sought and obtained injunctive relief that was affirmed on appeal by a divided court. 20

The defendants in both cases argued that the law of trespass to chattels did not allow suit in the absence of damage to the chattel, which was restricted to damage to its “condition, quality, or value,” none of which were directly implicated in these cases. The basic argument is wholly doctrinal in its appeal to the language of the Second Restatement. But as a functional matter, the claim appears to go astray at two levels: first, in their claim that the damages were solely nominal, and second, in their application of the nominal damage rule, which in principle has no place in cybertrespass cases.

In both these cases, the definition of nominal damages is far more expansive than its ordinary definition. If eBay or Intel had suffered only nominal damages, then why would either firm spend enormous sums of money in order to stop conduct that at some level they regarded as deleterious to their businesses? The central insight in the economics of litigation is that no plaintiff will sue to recover when the costs of litigation exceed the expected recovery of suit. But in this context the mystery disappears when the ordinary definitions of causation and damages are carried over from physical space to cyberspace. Even in cases of unintended entry, the plaintiff would recover harms that were caused directly, so long (at least in some versions of the rule) as the harm is foreseeable. Intended consequences are always foreseeable, so that the only question is whether the respective plaintiff can point to some form of consequential damages for which recovery is appropriate. These damages have been routinely allowed in cases of trespass to real property: “A trespasser is liable to respond in damages for such injuries as may result naturally, necessarily, directly and proximately in consequence of his wrong.” 21

These rules carry over to cyberspace without missing a beat. In *America Online, Inc v IMS*, 22 the court held that AOL's loss of good will when customers complained about the slow and balky operation of their service was an element of actionable damages, above and beyond any physical damage to the system itself. 23 Actions for trespass to real property have also allowed actions for consequential damages related to the distress of an occupant that is not attributable to the as-

---

20 See Hamidi, 114 Cal Rptr 2d at 246.
21 Bouillon v Laclede Gaslight Co, 148 Mo App 462, 129 SW 401, 402 (1910) (allowing recovery for nervous shock from defendant's servant's entry to property, even though plaintiff was not personally assaulted).
23 Id at *14 n 13.
sault of a wrongful entrant. In *eBay v Bidder's Edge*, eBay’s damages could easily include loss of good will if BE displays its listings incorrectly or in some unattractive format that makes its goods look inferior to those sold on others’ online auctions. The usual control of trade dress and appearance matters for ordinary store windows. It surely matters here. Likewise, employee distraction translates itself into poor morale, which in turn becomes lower productivity and lower profits. We do not have to estimate in the abstract how substantial these damages are because we have a perfect case of revealed preferences. The willingness of firms to sue in order to defend the exclusive use of their own space is evidence enough that the damages count. Even if these are difficult to estimate, we know that they are far greater than zero, so that the very inability to estimate the actual damages offers yet an additional reason to award injunctive relief. On this particular issue, the consequential losses should be estimated by the same rules that apply in physical space. The common law works itself pure by *not* adopting ad hoc rules when none are required.

The question of damages can also work in a second way. The usual rules of restitution hold that the plaintiff in a trespass action is normally entitled to choose between the benefits conferred on the defendant or the harm suffered by the plaintiff. In this case, the benefits to both defendants are hard to estimate. But difficult to estimate is one thing, nominal damages are quite another. With restitution damages as with tort damages, the difficulty in estimating substantial damages offers no reason to deny the injunction. It only proves that damages are inadequate as a matter of law. In a real sense, therefore, cybertrespasses do not require us to jettison the older requirement of actual damages. It only requires courts to interpret it sensibly in novel contexts that repeat familiar patterns.

C. Application of Trespass to Real Property to the Internet

The second point goes to analogy and comparison. Does a website look more like an ordinary chattel or more like real property? Thus far I have pursued the chattels line that has been followed in the cases. But, in principle, I think that the best answer comes from the descriptions of cyberspace offered by those who champion the distinctive nature of the cyber community, which appeals to an analogy drawn from ordinary understandings of real property. Common language speaks of internet “addresses,” for, of course, individuals and

---

24 See, for example, *Bouillon*, 129 SW at 402-03 (“[A]lthough the assault was not directed against plaintiff and no physical injury was inflicted in the first instance, defendant was liable to respond for such consequences as were proximate to his wrongful act.”), citing *Watson v Dilts*, 116 Iowa 249, 89 NW 1068 (1902).
firms occupy private "sites" along the internet "highway." It also speaks of the "architecture" of the internet, which may direct and influence conduct in both real and virtual "space."\(^2\) Reference is common to "cybersquatters." To think of a fixed internet site, or the equipment that supports it, as though it were a chattel or personal property is to miss the operative distinction of the earlier law, where "movables" was often used as a synonym for personal property and "immovables" as a synonym for real property. The blunt truth is that an internet site is fixed in its cyberspace location; to change from one address to another risks the loss of its customer base, just like any ordinary store runs the risk of losing its customers when it changes locations. In these circumstances, cyberspace looks and functions more like real property than chattels. If one is forced to choose between the two sets of rules, then manifestly the real property rules offer a better fit.

The basic issues involved in these cybertrespass cases can be put in yet another fashion. When the dust settles, if these defendants had been allowed to continue just as they are, then the upshot is that the defendant is entitled to receive an uncompensated compulsory license to use the equipment of the plaintiff for his own advantage. It takes little imagination to see that these cases therefore amount to the claim that property rules should give way to forced transfers of wealth. But in this case, much is lost in making this assumption. Our two cases of course involve very different situations. In *Hamidi*, there is no chance that Intel would ever enter into a deal that would allow Hamidi to send spiteful emails to its employees. Given that transaction costs are low, this is the correct result: There is no reason to allow Hamidi’s small gains to triumph over Intel’s large costs. The initial allocation of rights holds form. In *eBay*, the situation is different because auction aggregators like BE could work to the benefit of firms like eBay by making their goods known to customers in a wider market. But a lot depends on the terms and conditions of the license. Here, moreover, the actual eBay licenses in use at the time of the BE suit were complex affairs. The "eBay Deep Link, Trademark, Copyright, and Banner Ad Agreement," for example, in effect at the time of the BE litigation, ran for seven pages and contained, *inter alia*, provisions that govern how eBay licensees could "deep link" to the eBay site; the default display of eBay content on the licensee’s site; the protection and use of eBay’s intellectual property and advertisement content; basic compensation provisions including front end licensing.

\(^2\) See, for example, Lawrence Lessig, *Code and Other Laws of Cyberspace* 89 (Basic 1999) ("The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave.").
fees and additional payments from the auction aggregator for visits from its users to the eBay site and from eBay for each customer who registers with eBay when referred to it by an auction aggregator; restrictions on assignments and sublicensees; provisions governing termination and renewal of licenses; limitations on warranties for consequential damages; and provisions governing the cessation of services during emergencies. No compulsory license scheme, even with compensation, could hope to match the level of particularization and standardization achieved by contract.26 This is a great improvement over a rule that allows one person to take the property of another until the system crashes or slows down.

D. Beyond Basic Trespass Law

The arguments thus far have been designed to show why strong property rights for non-network elements function as well in cyberspace as they do anywhere else. In fact, both of these cases can be seen to raise issues that go beyond these points of trespass law. In eBay, for example, the defendant could argue that some limitation on eBay's ability to exclude was necessary to preserve a smooth-functioning competitive market in which information about relative prices flows quickly and easily between the parties. At one level, just that goal is achieved by the voluntary agreements that eBay entered with other auction aggregators. But in response it might be argued that eBay's refusal to deal on certain terms should count as anticompetitive behavior. But if that were the case, then what is needed is an action under the antitrust laws, not the trespass laws. That action will be hard to maintain. In the usual case the plaintiff alleges that the defendant had conspired to rig markets by some form of collective action. eBay has only refused to do business with one firm that offers both complement and substitute services on terms that it regarded as appropriate. So long as we do not require ordinary auction houses like Christie's or Sotheby's to allow any potential publicist to enter their showrooms, it is hard to see how this claim of an antitrust violation has much traction. But even if it does, it could be pleaded even if the ordinary rules of trespass to real property carried over to cyberspace.

Likewise in Hamidi, one argument was that virtually everyone who surfs the net will count as a trespasser, even in the absence of actual damages. Justice Kolkey put the point as follows: "If a chattel's receipt of an electronic communication constitutes a trespass to that

chattel, then not only are unsolicited telephone calls and faxes trespasses to chattel, but unwelcome radio waves and television signals also constitute a trespass to chattel every time someone inadvertently sees or hears the unwanted program. 27 But this argument is wrong in all its analogies. Take first the telephone calls and the faxes, which are sometimes a real annoyance. The missing pieces in the puzzle are the rules on consent. In the ordinary situation a powerful set of social expectations make it clear that ordinary phone calls and faxes are not trespasses, any more so than routine entries into department stores. The operative principle in these cases is that consent is implied from the circumstances until the owner of the property tells the entrant to stay off (if not on the premises) or leave (if he is). Certainly, websites that clamor for "hits" are widely understood to take all the ordinary traffic that they receive, and we have little reason to think that anything decided in Hamidi will reverse those expectations. But in this case, one defendant was told to keep off, and here the background expectations have been shifted by explicit instructions, which should be as binding in this context as they are in cases of entry to real property. The problem that Justice Kolkey posits disappears unless we have a tin ear to standard social practices. "Unwelcome" is an evasive word, but it is not a synonym for unauthorized. There are lots of phone calls and faxes that we would rather not receive. But there are relatively few that we have forbidden. Unwelcome advances are reasons for rebuff; but until the rebuff comes, the implied license continues to hold. Hamidi crossed that line in ways that many others do not.

The analogies to radio waves and television shows are similarly unavailing. The radio waves that run across the land do not pack any cognitive wallop. Insofar as they are just waves, they are prime candidates for the live-and-let-live rule of no liability, for everyone is better off if the waves can be sent than if they were all quieted. Radio and television signals that are heard and seen do pack a cognitive wallop and, thus, cannot be easily subsumed under the live-and-let-live rule. No doubt in most cases the ability to turn the knob will stop the trespass. But think of the reaction if rogue broadcasters were able to take over established frequencies in order to broadcast pornography into households where it was not welcome. Hamidi is just another kind of resourceful intruder. His case would never have gone to litigation if he had identified himself unambiguously on arrival to Intel's servers.

E. First Amendment Issues

The question then arises whether Hamidi's effort to send a message over Intel's server is protected by the First Amendment. First

27 Hamidi, 114 Cal Rptr 2d at 261 (Kolkey dissenting).
Amendment issues would loom very large if Intel had sued Hamidi for defamation. But the argument here goes not to the truth of his message but to the mode of its distribution. In this case, the court of appeals labored at great length over the question of whether the issuance of an injunction counted as a form of state action in light of the authority of *Shelley v Kraemer*, which held that a state could act (for an analysis under the Equal Protection Clause) through legislative, executive, and judicial action. That decision has always been very troublesome because it suggests that the only thing that does not count as state action is self-help—the very remedy that has proved inadequate to keep Hamidi’s emails from invading Intel’s servers.

The court of appeals sought to avoid this difficulty by noting that the neutral application of the general trespass law did not count as a form of state action. That denial seems a bit forced linguistically, because what is really being said is that the state action in question is justified because it counts as a neutral application of the trespass law. The point can, however, be made still stronger when it is noted that the decisive feature of private remedies is that they are sought by private parties. The entire question of monopoly force that troubles the application of state rules disappears from the equation except in those rare situations like *Marsh v Alabama* where it is difficult to draw the line between the state and the private owner of property that looks (at least in some ways) to possess an unusual level of a local government.

But in this case the decisive precedent is *Rowan v United States Post Office Department*, which upheld a legislative rule that applied to “pandering advertisements,” under which “a person may require that a mailer remove his name from its mailing lists and stop all future mailings to the householder,” noting that the right of privacy allowed the householder to be “the exclusive and final judge of what will cross his threshold.” This rule certainly allows an owner to keep peddlers and hawkers off his property. As the Court wrote, “To hold

---

28 See id at 253–55.
29 334 US 1, 14 (1948) (“[A] State may act ... either by its legislative, its executive, or its judicial authorities; and the prohibitions of the [fourteenth] amendment extend to all action of the State denying equal protection of the laws”), quoting *Virginia v Rives*, 100 US 313, 318 (1880).
30 See *Hamidi*, 114 Cal Rptr 2d at 253–54.
31 326 US 501, 509 (1946) (holding that Gulf Shipbuilding Corp, which owned all the property in the town of Chickasaw, Alabama, could not prevent religious activity on its property).
32 397 US 728, 738 (1970) (holding that a vendor has no right to send unwanted material into the home of another).
34 *Rowan*, 397 US at 729, 736.
less would tend to license a form of trespass and would make hardly more sense than to say that a radio or television viewer may not twist the dial to cut off an offensive or boring communication and thus bar its entering his home."

Households are of course not businesses, but the differences do not matter in the grand constitutional scheme of things. The household in Rowan did not want the mail delivered to his home for fear that it would find its way into the hands of minor children, which is the same sort of consequential damages applicable here. The general common law right to exclude is not, of course, confined to pandering materials, but extends to any information whatsoever. Because there is no general pressure to prevent the delivery of ordinary mail, the statutory protections did not authorize its interception by the Post Office. But it hardly follows that the individual householder could not communicate to any particular person that he should not deliver any mail to his home. Delivery, after notice, would count as a trespass, even in the absence of a mechanism that allows the Post Office to refuse to deliver the mail in the first place.

I can see no reason why the principles of exclusion that apply to households do not apply to businesses as well. It is common practice in many businesses to limit the connections that workers can make to and from the firm. So long as these restrictions are spelled out as part of the general employment relation, they do not amount to the infringement of any right of any employee to receive or deliver mail. Hamidi remains free to send his mail to Intel employees anywhere else. But he is denied the convenience of using their servers to reach this end. If the state can use its legislative power to assist personal owners in protecting themselves against the intrusions of others, then it seems as though they should be allowed to use the judicial agencies of the state to the same end. To reach any other conclusion would be odd in the extreme: Who would forfeit political power to the state if the legal remedies it supplied in exchange were worthless? So long as self-help is available in principle, then an injunction should be available to back it up.

CONCLUSION

In the end, therefore, a case as "simple" as cybertrespass leads us down all sorts of strange paths. But it also confirms Kalven's original insight about how the law works itself pure. There are many false turns that can be taken, and many technical and doctrinal complexities that can be injected into cases of this sort. In some circumstances we do need to modify traditional right situations to deal with new

35 Id at 737 (emphasis added).
forms of property rights. But that proposition is not some unarticulated but universal truth. Sometimes the old analogies work just fine. So long as we keep our eye on the ball, we do not have to be fearful of the imagined consequences that will follow by taking the older rules of trespass and carrying them over to the brave new world of cyber-space, which, when all is said and done, for legal purposes at least, is neither as brave nor as new as it first appears.
The Self-Defeating International Criminal Court

Jack Goldsmith†

Great expectations greeted the opening of the International Criminal Court (ICC) on July 1, 2002. Kofi Annan captured these expectations when he expressed the hope that the new ICC would "deter future war criminals and bring nearer the day when no ruler, no state, no junta and no army anywhere will be able to abuse human rights with impunity." Chris Patten, the European Union Commissioner for External Relations, echoed this theme when he stated that the new Court's purpose was to "ensure that genocide and other such crimes against humanity should no longer go unpunished." Scores of other world officials, human rights activists, and international law experts made similar predictions.

These are unrealistic dreams. They are unrealistic for many reasons. But perhaps the most salient reason is that the ICC as currently organized is, and will remain, unacceptable to the United States. This is important because the ICC depends on U.S. political, military, and economic support for its success. An ICC without U.S. support—and indeed, with probable U.S. opposition—will not only fail to live up to its expectations. It may well do actual harm by discouraging the United States from engaging in various human rights-protecting activities. And this, in turn, may increase rather than decrease the impunity of those who violate human rights.

I lay out the mechanisms of ICC futility and perversity as follows. Part I shows why the ICC will be incapable of punishing serious human rights abusers. Part II shows how the ICC will likely lead to less rather than more punishment for human rights abusers. Part III asks why the ICC framers might have designed a self-defeating institution. The Conclusion qualifies the analysis and points to larger lessons.

† Professor of Law, The University of Chicago. Thanks to participants at workshops at the University of Chicago Law School and the University of Virginia School of Law, and to Curtis Bradley, Rosa Ehrenreich Brooks, Ryan Goodman, Jim Haynes, Derek Jinks, David Martin, Duncan Snidal, Peter Spiro, Paul Stephan, and Adrian Vermeule for helpful comments, and Mark Mosier for outstanding research. This Essay was completed before Professor Goldsmith took a leave of absence to serve as Special Counsel to the General Counsel of the U.S. Department of Defense. The views expressed in this Essay are those of Professor Goldsmith and do not reflect the official policy or position of the Department of Defense or the United States Government.

1 Marlise Simons, Without Fanfare or Cases, International Court Sets Up, NY Times A3 (July 1, 2002).
2 Chris Patten, Why Does America Fear This Court?, Wash Post A21 (July 9, 2002).
I. FUTILITY

The ICC was created in 1998 at an international conference dominated by weak and middle powers and by nongovernmental organizations (NGOs). The Court has jurisdiction over genocide, crimes against humanity, war crimes, and (at a later date) aggression. As the opening quotations suggest, the ICC's aim is to punish and deter individual perpetrators of these crimes.

The ICC founders hoped to minimize political influence over ICC decisionmaking. The ad hoc tribunals for the former Yugoslavia and Rwanda were created by the UN Security Council. The United States argued in Rome (the site of the ICC's founding conference) that ICC prosecutions should be similarly limited to cases referred by the Security Council. But the prevailing parties in Rome believed that the Security Council—and in particular the opportunistic votes of veto-wielding permanent members—was part of the problem. They believed the Security Council's failure to establish international tribunals for crimes in other trouble spots demonstrated that a Security Council gatekeeper would preclude legitimate prosecutions and thus undermine the aim of universal justice. Even worse, the permanent member veto would make the permanent five (U.S., France, United Kingdom, Russia, and China) and their close allies immune from prosecution.

The ICC founders thought that the selective justice inherent in such big-power politics would discredit the ICC process. So over U.S. objections, they created a prosecutor and court with powers entirely independent of the Security Council. To be sure, the ICC treaty gives the Security Council concurrent power to refer prosecutions to the ICC. It also gives the Security Council the power to delay a prosecution for twelve-month renewable terms. But this latter provision, if successful, marks a significant change in the architecture of international politics. It reverses the burden of Security Council inertia by

3 The main force at the conference was a group of sixty “like-minded” nations made up primarily of European and commonwealth countries. See William A. Schabas, An Introduction to the International Criminal Court 15 n 53 (Cambridge 2001) (listing countries). The like-minded nations insisted on two of the ICC's core, and controversial, features: the diminution of a Security Council veto and an independent prosecutor. See id at 15. So too did the over eight hundred NGOs represented at the conference.

4 See also Rome Statute of the International Criminal Court (ICC) preamble §§ 4–5, online at http://www.un.org/law/icc/statute/english/rome_statute(e).pdf (visited Jan 10, 2003) (“Affirming that the most serious crimes of concern to the international community as a whole must not go unpunished and that their effective prosecution must be ensured by taking measures at the national level and by enhancing international cooperation.”).


6 ICC Art 13(b).

7 ICC Art 16.
permitting an ICC case to go forward as long as a single permanent member supports prosecution and thus vetoes any delay. More broadly, it means that an international institution not beholden to the Security Council will have decisionmaking power over many of the same peace and security issues typically governed by the Security Council alone.\(^8\)

The ICC can exercise its independent jurisdiction over perpetrators of international crimes if the crimes are committed (a) by a national of a signatory party, or (b) on the territory of a signatory party.\(^9\) Two important consequences follow. The first is territorial liability over non-signatories. The ICC has jurisdiction over crimes committed by a non-signatory nation in the territory of a signatory nation. The second is the traveling dictator exception. Leaders of non-signatory nations can commit crimes in their territories without fear of prosecution. Even if human rights abusers from non-signatory nations vacation in The Hague, they cannot be arrested and tried by the ICC.

Why would the ICC founders reject jurisdiction over non-signatory nations who commit crimes in their own territory, but embrace jurisdiction when those countries commit a crime in the territory of a signatory nation? This result was a compromise. Many nations wanted the ICC to have universal jurisdiction, which would have abolished the traveling dictator exception by allowing any signatory nation to arrest anyone who committed an international crime anywhere. But other nations objected to universal jurisdiction as having an uncertain basis under international law and as an excessive threat to national sovereignty. The United States went further, objecting both to universal jurisdiction and to non-signatory liability for crimes committed in a signatory nation. Most nations in Rome disagreed with the United States. The final compromise—one designed both to satisfy some U.S. objections and to maximize ratifications—jettisoned the relatively controversial universal jurisdiction idea but retained the relatively (but only relatively) uncontroversial non-signatory liability for crimes committed in a signatory state.\(^10\) The framers also went further in the direction of non-signatory liability by allowing a non-signatory nation to consent to the ICC’s jurisdiction with respect to


\(^9\) See ICC Art 12(2).

\(^10\) The latter idea is relatively uncontroversial because it is premised on a signatory state’s territorial jurisdiction, which is delegated to the ICC. The delegation component is novel, but territorial jurisdiction over crimes is not. For a more critical perspective on the delegation component, see Madeline Morris, *High Crimes and Misconceptions: The ICC and Non-Party States*, 64 L & Contemp Probs 13, 43-47 (2001).
"the crime in question" committed on its territory by another non-signatory nation."

This is the fatal compromise that I believe will ensure that the ICC fails in its aim of ending—or even diminishing—impunity for international crimes. One reason why is obvious. The most salient class of human rights violators during the past century has been oppressive leaders who abuse their own people within national borders. Under the traveling dictator exception, the ICC does not touch this class of offenders, even if they travel abroad. Unless oppressive regimes ratify the ICC (something few are expected to do), the ICC simply fails to address the most serious human rights abuses.

There is an important qualification to the traveling dictator exception. If the Security Council refers a case involving an ICC non-signatory to the ICC under Chapter VII of the UN Charter, it can override national sovereignty and legitimate a prosecution against a non-signatory or some other state otherwise outside ICC jurisdiction. However, such a referral remains subject to the permanent member politics that so worried ICC supporters. And even when Security Council inertia can be overcome for purposes of establishing ICC jurisdiction, the ICC itself lacks the institutional resources to ensure that the defendants actually show up in The Hague.

Notorious human rights abusers tend to hide behind walls of national sovereignty, where they are hard to reach. Even with a Security Council referral, the ICC is unlikely to punish the Husseins and future Milosevics of the world because it is unlikely to get its grip on them. The ICC has no inherent enforcement powers. It depends completely on member states to arrest and transfer defendants. So the efficacy of even Security Council-initiated prosecutions in this context depends on the uncertain resolve of nations to use military or economic force to extricate an oppressive leader from his country.

Consider the experience of the International Criminal Tribunal for the former Yugoslavia (ICTY) in The Hague. The Tribunal has had modest success in trying war criminals, and it is currently prosecuting

1 ICC Art 12(3) (cited in note 4). The ICC Preparatory Commission has tried to soften this provision with its Procedural Rule 44(2), which provides that a State filing an Article 12(3) declaration "[accept[s] ... jurisdiction with respect to the crimes referred to in Article 5 of relevance to the situation." ICC Rules of Procedure and Evidence Art 44(2), online at http://www.un.org/law/icc/precottom/precфе.htm (visited Jan 10, 2003). This vague provision does not, as many have stated, guarantee that Article 12(3) parties will consent to jurisdiction for all crimes related to the consent. But even if it did, the Iraqs of the world could consent under Article 12(3) and simply not show up. Rule 44(3) improves the anomaly of Article 12(3), but does not fix it.

12 See ICC Art 13(b).

13 The analysis that follows also applies to leaders of signatory states that commit human rights abuses but do not travel abroad.
Milosevic. But it was not the gravitational pull of the ICTY Charter that lured these defendants to The Hague. Rather, it was U.S. military, diplomatic, and financial might. U.S. military and diplomatic power ousted Milosevic's and other unattractive regimes in the Balkans, making a trial of Balkan leaders a possibility. And it was the United States's threat to withhold a half-billion dollars in U.S. and International Monetary Fund (IMF) aid to the successor regime in Yugoslavia that led to Milosevic's actual transfer to the ICTY.14

The ICTY example illustrates the importance of military and economic force to international criminal justice when human rights abusers hide behind national borders. It also illustrates the obstacles to the use of such force. Nations do not lightly expend national blood and treasure to stop human rights abuses in other nations. The Europeans were unwilling and unable to do so in the Balkans for years. When the United States finally used extensive force in Kosovo in the summer of 1999, it did so haltingly and in large part to protect the viability of NATO. The United States did not intervene to stop equal or greater humanitarian tragedies in Chechnya, Rwanda, and Sierra Leone. The brute fact is that despite hundreds of thousands of deaths caused by human rights abuses during the past decade and despite millions of such deaths in the last century, no wellspring of support for intervention has developed in the industrialized democracies that possess the military muscle to intervene and stop the abuses.

Bringing the most notorious human rights abusers to the ICC would thus be hard enough even if the United States fully supported the ICC. But for reasons we shall explore below, the United States does not support the ICC. It openly and aggressively opposes it. The United States’ opposition will greatly magnify the ICC’s inherent enforcement gap. The United States can sometimes be persuaded to engage in humanitarian intervention if the intervention comports with certain strategic interests. The leading contender to replace the United States as world policeman, the European Union, lacks the budgetary and political will to conduct any serious military actions outside Europe. (Despite much talk in recent years, there is no foreseeable prospect of the EU transforming itself to do otherwise.) So at best, ICC power over recalcitrant oppressors will depend on uneven enforcement efforts by the United States when it suits U.S. strategic interests (and when—if ever—the United States can overcome its objections to ICC participation). It is much more likely that the ICC will fail to assert jurisdiction over recalcitrant oppressors at all, either be-

cause it lacks a Security Council referral and thus will lack jurisdiction, or because no nation will be willing to bring the defendants to The Hague.

These are the main reasons why the ICC is not likely to end impunity for human rights abusers or deter future war criminals. Of course, even if the ICC cannot try big-time human rights abusers, it might be able to try less significant ones. There may be times when signatory states (Nigeria and Sierra Leone are two possibilities) have civil wars that involve gross human rights abuses, and in which the prevailing or successor regime sends the defeated party to the ICC. Or there may be a cross-border dispute in which a signatory captures a perceived war criminal and sends him to The Hague.

These are the most likely possibilities, but they are far from certain. In the civil war context, victors will not lightly send losers to the ICC for fear of dampening national conciliation efforts. (Recall that the post-Milosevic regime sent Milosevic to The Hague only in the face of extraordinary U.S. financial and diplomatic pressure; the Yugoslav government's decision to do so was unconstitutional under domestic law, and continues to divide rump Yugoslavia today. International tribunals are not, as a general matter, viewed with favor by regimes that succeed oppressors.) When the losers are so broadly detested that an ICC transfer seems desirable, the ICC's additional penal effect is minimal. A similar analysis applies to potential defendants captured during cross-border wars. And in any event, cross-border wars have not been the primary source for massive human rights abuses in modern times; and any such abuses are not likely to involve the self-selected ICC signatories.

I am not arguing that the ICC will have no effect whatsoever. Surely it will. As the Palestinian response to Israeli military attacks in July 2002 indicates, it will be a focal point for rhetorical assertions about criminality even in cases in which the ICC clearly lacks jurisdiction. And its existence will make it easier (though perhaps not much easier) to pressure signatory nations to turn over alleged human rights abusers in their jurisdictions. The ICC will gather its share of defendants—especially low- to mid-level human rights violators from signa-

---

18 See Harvey Morris, Legal Move to Halt Israeli Assassinations, Fin Times 13 (July 26, 2002). The ICC clearly lacks jurisdiction over this case because the occupied territories are neither a state party to the ICC nor a state capable of an Article 12(3) declaration.