

Internet Law

Professor Grimmelmann

Final Exam - Fall 2008

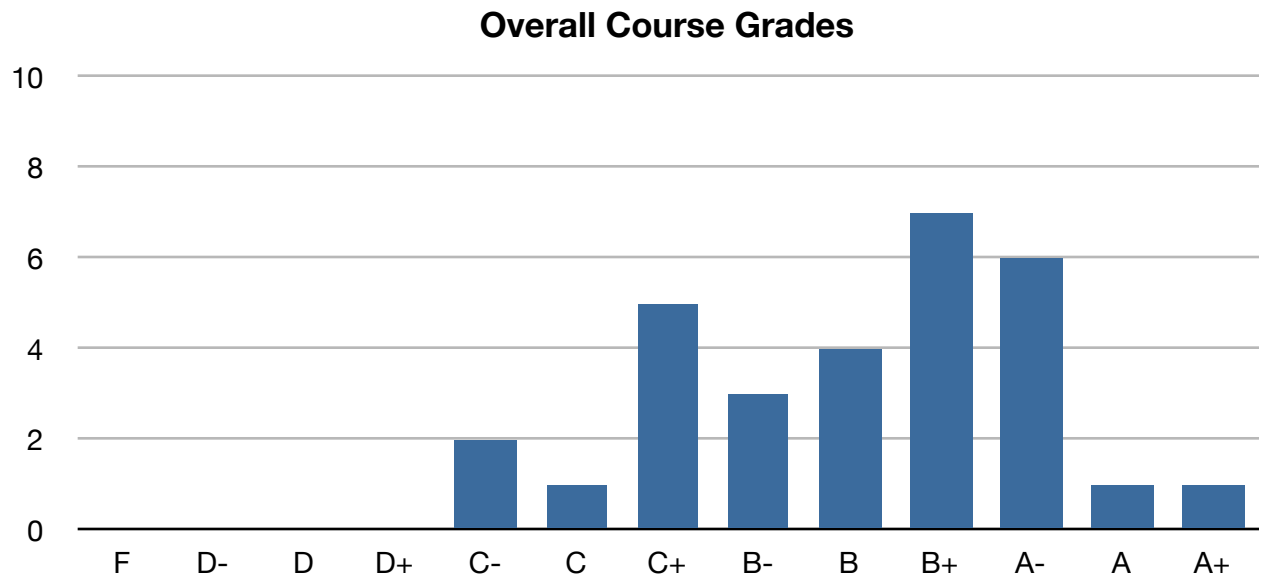
This exam was hard. The first question raised difficult borderline doctrinal issues; the question asked you to extrapolate familiar doctrines to an unexpected fact pattern; the third required a great deal of practical judgment. All three are characteristic of Internet law practice.

I graded the three problems by creating a thirty-three-item checklist for each. You got a point for each item (e.g. “Exploitr is an interactive computer service under Section 230.”) you dealt with appropriately. I gave out frequent bonus points for creative thinking, particularly nuanced legal analyses, and good use of facts.

If you’d like to discuss your exam, the course, or anything else, please email me and we’ll set up an appointment. If you have exam questions, please read through this memo before getting in touch. It’s been a pleasure and a privilege to teach you and learn from you. May you enjoy the best of luck in your future endeavors!

James

	Exploitr	Bananaphone	Ultrimpex	Total
Average	19.2	18.3	16.2	54.7
Median	19.0	18.5	16.5	55.0
Std. Dev.	4.3	4.4	3.3	8.6



(1) **Little Photoshop of Horrors**

It was easy to see which end was up on this problem; Frank Matasar, Flawless 8, and the New York attorney general might potentially give Exploitir a hard time. This also gave the analysis a natural structure—by possible plaintiff—which all of you followed. Your job was to look for defenses Exploitir could use and evaluate whether they applied or not. Everyone in the class was also able to do that.

The problem got tricky in the details; Exploitir’s technical operations are structured in a way that makes it hard to just pull doctrines off the shelf and apply them. As always, the best answers were the ones that read the facts closely and fit the analysis to them, rather than just reciting tests and doctrines. I was happy that you embraced your role as counselors. Most exams gave Exploitir practical, as well as legal, advice. Some of it was quite good.

Frank Matasar

I wanted you to start from the seemingly obvious point that Frank Matasar potentially has a viable defamation claim. On the present factual record, it’s impossible to say much more than that. (The facts also suggest a possible false light claim, but New York doesn’t recognize a false light tort. *See, e.g., Costanza v. Seinfeld*, 693 N.Y.S.2d 897 (Sup. Ct., N.Y. Co. 1999). All of this is largely beside the point, since this is an Internet Law class, not Advanced Torts.)

Matasar is likely to want to sue the unknown third party who created the doctored photo—and to come to Exploitir to learn his or her identity. Be prepared for a subpoena seeking that person’s IP address. A few answers went further and explained that the Stored Communications Act posed no bar to Exploitir’s disclosing the user’s IP address.

If Exploitir is the defendant. Section 230 provides an obvious defense. Exploitir is clearly an “interactive computer service.” The hard part is whether the defamatory material was “provided by another information content provider.” As the courts have interpreted that issue, it turns on Exploitir’s participation in the creation of the content. In the *Roommates.com* formulation, Exploitir can be found liable where it “contributes materially to the alleged illegality of the conduct.”

This is a hard, subtle issue. What I hoped you’d see is that it’s not just the user vs. Exploitir who could be the provider” of the content, but also Exploitir vs. the third-party web sites from which it pulls the content. Key facts here would include, on the one hand, that Exploitir specifically chooses the “flawless 8” search term and specifically combines heads and bodies, and on the other, that the search is driven by Google and the choice after the search is random. A court might find that the third-party sites are the relevant source of the defamatory content, or that a court might hold Exploitir responsible. I gave full credit for either answer, as long as you were specific about the facts involved.

Trademark

Flawless 8 may sue Exploitir for trademark infringement. It won’t win. Yes, Exploitir “uses” the trademark in the sense that it conducts a search using it. But the trademark is never shown to

users, on the facts as given. This is an even better case for the defendants than *Rescuecom*; there, users typed in the trademark as a search term, so they were arguably exposed to it. *Brookfield* is distinguishable; there, consumers were searching for the trademark. Here, consumers aren't aware the mark is in play at all, so there can be no use as a trademark and no consumer confusion.

Many of you worried about whether users might be shown the trademark as a watermark in the photos. That's a sensible, factually grounded worry, and I gave some credit for asking that question. I didn't hand out additional points for asking whether Exploittr showed users the trademark in other ways; nothing in the problem said that it did.

Copyright

Many of you gave reasonable answers on many of the copyright doctrines we studied, but strung them together in ways that make no sense under copyright law. For example, I saw several times answers that went through the fair use factors, concluded that Exploittr has a strong fair use defense, and then said something like, "Even if Exploittr has a fair use defense to direct infringement, we must still consider contributory and vicarious liability." That's copyright crazy talk; if you have a fair use defense, it shields you from all copyright liability, direct and indirect. I deducted no points for mistakes of this sort; this wasn't a copyright course, and the framework takes time to learn. I expected you to know only the doctrines we actually studied. And as it turns out, to answer this problem well, you needed to discuss most of them.

The place to start was in looking at the elements of infringement. The fact that Exploittr deletes the composite images within 30 minutes from its servers suggests a possible defense that the images are never "fixed." *MAI v. Peak*, however, disposes of that defense. Exploittr has *prima facie* violated the reproduction right. I also hoped you'd note the *London-Sires* issue with the distribution right, and some of you did; a jury could conclude that Exploittr distributed the copyrighted photo to the public because some unknown person downloaded it.

Exploittr could argue that its infringement wasn't "volitional" under *Netcom*, because it fetches the copyrighted images as the result of an automated process. That sounds right at first, but I doubt the *Netcom* court would go there, because one might find the necessary volition in setting up the search term. Here's a possible analogy. The owner of a copy machine who makes it available to the public doesn't have volition as to the books people copy using it. But the owner of a copy machine who puts a copyrighted book face down on the glass and then makes the machine available does have volition as to the photocopies people make of that specific book,

Even if Exploittr isn't volitional, it potentially faces indirect liability. On contributory liability, material contribution is easy, since Exploittr itself makes and distributes the copies. I'm not sure about actual knowledge, but imputed knowledge is also pretty plausible, since Exploittr is presumably aware that many of the search results on a search for "flawless 8" will be copyrighted and might be expected to know that some of those results will be infringing. A *Sony* defense is inapplicable here; Exploittr is a service, rather than a device, and has the kind of ongoing control that Napster did. Vicarious infringement might succeed; Exploittr has the ability to control infringement (use a different search or shut down), but financial benefit will turn on the same

exact issues at stake in *Napster*. Finally, one might point to Exploitr's name and business model in finding that it induced its users to infringe.

Exploitr might raise a 512(c) defense. (If you thought 512(a), (b), or (d) would work, you missed a key fact from the problem or you misread the statute.) Both the vicarious and contributory infringement analyses above could knock out the 512(c) defense, however. It's also not clear that the infringing copies are being stored "at the direction of a user."

Finally, Exploitr may have a fair use defense. I thought that the most interesting questions here were whether the use was transformative (the photo compositing is an interesting twist), whether the use is commercial (or might be, if Exploitr starts charging), and whether this kind of photoshopping illegitimately harms the market for Flawless 8 photos. *Perfect 10* was a good starting point for this analysis.

The New York Law

There's an obvious threshold question as to whether Exploitr's use here is "commercial." Assuming that it is, Exploitr meets all the other requirements to violate the statute. Thus, Exploitr might face prosecution. Some answers suggested that Matasar could sue under the statute. He can't; it's a criminal statute and the problem says nothing about it creating a civil cause of action.

The first objection to interpose is that § 230 preempts this law. Good answers said that it did. (Only *federal* criminal laws are saved from 230's reach, and it's extremely hard to argue that this is an intellectual property law, given that it turns on indecency and that it's criminal.) Excellent answers pointed out that the preemption analysis is nearly identical to the analysis of whether Matasar's tort suit is blocked.

The second issue here is that this law may have constitutional infirmities. There's a possible First Amendment issue with the law's restrictions on speech, and "indecent according to community standards" is typically not a phrase that the *Miller* test would look kindly upon. But perhaps the other requirements, especially the one about an identifiable individual, might save it. I didn't require any extended analysis here; saying as much as I just have would have put you in bonus-point territory. You could also flag the Dormant Commerce Clause issue. I don't know that New York could constitutionally apply this law to protect out-of-staters, but to protect its own residents . . . again, I didn't ask for a definitive answer, just that you flag the issue.

Jurisdiction

I didn't care about jurisdictional analyses. I didn't mark you down for them, but if you started talking about personal jurisdiction over Exploitr, I skimmed ahead until you stopped, and then started reading again. First, the problem never tells you where Exploitr is located. Second, so what if you win the jurisdictional analysis as to Matasar or Flawless 8? They can just sue you in another state. (As counsel for a potential defendant, you will almost never care about personal jurisdiction *unless* you are trying to dismiss a lawsuit already filed.) Third, any objections to personal jurisdiction in resisting the New York law will also be available in the Dormant Commerce Clause analysis.

Strategy

The first thing to catch is that Exploitr's decision of whether to start charging affects a lot of its defenses. If it's "commercial," it's one step closer to liability on trademark infringement, vicarious copyright infringement, fair use, and the New York statute. That's a reason to counsel it not to start charging. I gave you a point for saying so. It's also *terrible advice*. Exploitr is a business; it needs to find a way to make money. If it's not charging \$1.00 a permalink, it'll be something else. Staying noncommercial forever is almost certainly not a realistic option. This is one reason why entrepreneurs often look down at lawyers; the lawyers aren't sensitive to business realities. Now, sometimes you do need to be the one throwing cold water on your client's legally outrageous plan. But whenever possible, look for ways to help your client meet its objectives while also minimizing legal risks.

Thus, the second thing to notice is that Flawless 8 is a terrible enemy to have; they're apparently a very litigious company. There's an easy fix here: stop ripping off their copyrighted images. Exploitr's business model is about making funny and/or offensive composite photos; the words "flawless 8" don't need to appear in there at all. Just go out and license some photos from a copyright owner (possibly even Flawless 8) or commission some of your own. There you go: you can eliminate step 4 from the process, and with it, most of Exploitr's potential copyright liability.

The third thing to take care of is to clear up some of Exploitr's unnecessary § 230 risks. Right now, the site's design directs users towards a specific kind of nasty photoshopping. If the site becomes less directed—e.g., users simply upload both photos, without prompting as to what they should be—its § 230 defense under *Roommates.com* becomes stronger.

Finally, even though this isn't strictly speaking legal advice, perhaps Exploitr should get into a more ethical line of business.

Question Sources

Exploitr is loosely based on a hypothetical in the first, withdrawn, *Roommates.com* opinion, with elements of various Google mashups thrown in. Its name is a play on Defamer.com and on Flickr.com. Flawless 8 is a lighter isotope of Perfect 10, and some of the "not stored here" angles are borrowed from the *Perfect 10* case, though used to different effect. In old photos of Dean Matasar, his mustache looks as though it was Photoshopped in.

(2) **Ping Ping Ping Bananaphone**

Don't you just love how the same few facts can have consequences under so many different bodies of law? Welcome to Internet Law. I gave you the parties' various pleadings as a hint; their claims direct you to the appropriate areas for analysis. I meant for the preliminary-injunction setting to make your life easier, as well; if there aren't sufficient facts to reach a conclusion, you can tell the judge to ask for them. Many of the facts that are in the problem can be used cleverly in multiple places; it was generally sufficient for full credit if you made reference to each fact on at least one appropriate point. Overall, you did solidly here. Many answers handled each legal issue competently, though there was enormous diversity in the class as to which issues you really nailed.

Trespass to Chattels

The threshold question here is what is the chattel? "Bandwidth" is an abstraction, not personal property. Metro Cable's routers are the relevant personal property, which means that we care about whether BananaPhone interfered with Metro Cable's ability to use the routers or damaged them. *eBay* would seem to support a finding that it did; 25% of its total load is enormous, and it's easy to see how service would be seriously degraded if other video-chat systems used up similar amounts. The facts that BananaPhone started evading Metro Cable's blocking and sending even more redundant packets are also bad for BananaPhone. It's also unquestioned that BananaPhone's use was unauthorized, thanks to the letter Metro Cable sent it.

On the other hand, *Hamidi* would say that Metro Cable can't sue unless its possessory interest was really interfered with. The problem never says that Metro Cable's network has actually slowed down, or that its servers have crashed, or that the increased traffic ever increased its costs. On the present state of the factual record, Metro Cable isn't entitled to relief. Judge Harlan should ask about impairment at oral argument.

I gave full credit whether you found *eBay* or *Hamidi* more persuasive, provided you noted that both were plausible precedents and noted the relevant facts under each. One possible way of distinguishing them was to say that *Hamidi* turns on the free speech angle, and to ask whether there's a similar free speech angle here. Perhaps not: BananaPhone's use of the Metro Cable network seems purely commercial.

One last twist here involved the intentionality of the trespass. Some of you, citing *Universal Tube*, said that it's BananaPhone's users who use the Metro Cable network when they use BananaPhone, not BananaPhone itself. The problem with that argument is that BananaPhone's return messages to each user come from BananaPhone itself. A few answers correctly pointed out that BananaPhone faces a hard problem if it tries to filter out traffic to Metro Cable customers; it can't easily tell who they are. (Perhaps Metro Cable could help it out with that . . .)

Computer Fraud and Abuse Act

Just like trespass to chattels, only different! Plug through the issues we discussed in class, in order, and you'll do fine.

Metro Cable’s routers are “protected” since they’re used in interstate commerce—Metro Cable itself is multi-state.

BananaPhone “accesses” those routers when it sends messages to Metro Cable customers. There’s (probably) no *Allen* issue because routers don’t have anything like a login; they just route packets.

“Authorization” is, as always, the hardest issue. On the *Morris* intended-function test, BananaPhone used the routers for their intended function: to route packets. That’s not unauthorized. On the no-account test, one doesn’t need an account to route packets. Again, not unauthorized. (Or, alternatively, Metro Cable’s customers do have accounts, and gave BananaPhone access, *Konop-style*.) On the *Shurgard* test, Metro Cable didn’t approve, and therefore the access was unauthorized.

Finally, damage or loss raises the same factual issues as the impairment issue under trespass to chattels. There are tricky statutory-interpretation issues here, though I didn’t require you to get into the details at all. Two of you cleverly asked whether BananaPhone “cause[d] the transmission of a program, information, code, or command,” 18 U.S.C. § 1030(a)(5)(A)(i).

Breach of Contract and Tortious Interference

It made sense to discuss these together. Metro Cable uses clickwrap for its user agreements; on the facts you have, the users are clearly bound. *ProCD*. Space spent speculating about whether the contracts were properly shown to users was generally wasted. BananaPhone, however, is not a subscriber to Metro Cable on the facts given in the problem. As such, it is not a party to the clickwrap agreement, and is not bound by it. End of story.

Or is it? Metro Cable did send that letter. Perhaps the *letter* could be considered the contract, so that BananaPhone is on notice of the demand to stop using the network. This theory of the contract probably also fails, for at least two reasons. First, there’s nothing in the facts you have to say that the letter claimed it was offering a contract. Second, it’s hard to argue that BananaPhone’s continued use of the network could reasonably be construed as acceptance. (BananaPhone’s name was a very subtle hint at the banana+subway hypothetical from class on what actions could be construed as acceptance.)

Even if BananaPhone isn’t itself breaching a contract, perhaps it’s tortiously interfering with Metro Cable’s subscriber contracts. One theory here is that BananaPhone is inducing users to breach those contracts—presumably the “expressly permitted” term. (But since that term would seem to make almost all use of the network forbidden, perhaps Metro Cable should be treated as having waived it.) Or perhaps it’s inducing them to violate the “tortious or criminal” clause of the contract—the prank phone calls might be relevant here. An alternative theory, though one largely subsumed by the trespass to chattels argument, is that BananaPhone is preventing Metro Cable from fulfilling its obligations to its subscribers.

Turning things around, is Metro Cable interfering with BananaPhone's own contracts? The problem is silent about what contracts those might be, but it's not hard to assume that its user contracts or its advertising contracts could count. (Even if there aren't contracts, they might be prospective business relations, so we're in the same tort family.)

The hard part on both of these theories is articulating a reason why either Metro Cable or BananaPhone's actions are wrongful! None of you went particularly deep here, but that's okay: this is the embarrassing part of tortious-interference doctrine itself. One clever twist is to borrow from *Search King* and ask whether either BananaPhone or Metro Cable might raise a plausible argument that its activities can't be wrongful because they constitute protected First Amendment activities.

Wiretap Act

Almost everyone understood that the issue here is whether Metro Cable has "intercept[ed]" messages to or from BananaPhone. Not everyone grasped what "intercept" means in the Wiretap Act: "*acquisition of the contents* of any wire, electronic, or oral communication" (emphasis added). Metro Cable would have to find out what the message says to violate the Wiretap Act, so just preventing the message from getting through isn't a Wiretap Act violation.

Dig deeper, though. How does Metro Cable know which messages to block? Does it have to engage in deep-packet-inspection to do so, and would that mean that deep packet inspection is a Wiretap Act violation, as Paul Ohm claims? Fortunately for Metro Cable, the addressing information is the only part of the packets it needs to look at. Recall our discussion of trap-and-trace/pen registers; addressing information isn't the "contents" of a message. So it looks like Metro Cable could be okay, but this is an issue to press them on at oral argument. (Alternatively, how exactly does Metro Cable know that BananaPhone is used to place prank phone calls?)

Clever answers here also appealed to the subscriber-consent and provider exceptions in the Wiretap Act. Ohm spends substantial parts of his analysis examining these exceptions, and neither of them yields a clear-cut result.

Network Neutrality

Blocking packets based on their destination for purely commercial reasons is the core example of a network neutrality violation. It's even more discriminatory than blocking a protocol, as in the Comcast case heard by the FCC. So this is a clear-cut violation . . . and Judge Harlan can't and shouldn't do anything about it. After *BrandX*, there is no judicial authority for anything remotely resembling network neutrality; the FCC's new policy is an FCC matter only.

Preliminary Injunction

I didn't ask for much here, but I did ask for something. The problem put you in a specific role, and the judge wants to know whether to grant either side an injunction. I gave full credit for any answer that was supported by your analysis above. Point out the irreparable harm (or lack

thereof) and point out which side (if either) is likely to succeed on the merits of its affirmative claims.

Question Sources

Believe it or not, this question was inspired by the Lori Drew case! I started off trying to figure out whether someone could get in deep trouble based on the terms of service of an ISP they'd never heard of. The question went through many drafts and eventually evolved into its present form: essentially a network neutrality dispute in which the terms of service play a disproportionate role. As for the names, Bananaphone is a Raffi song alluded to in the problem name, and Metro Cable is not the name of any actual ISP. John Marshall Harlan, NYLS '24, would have approved of leaving the contentious network neutrality debates to the FCC, rather than trying to resolve them in court.

(3) **Pirates of the Domain Name System**

This question was a bit of a Rorschach blot. Was Ultrimpex the victim of a clever *Kremen v. Cohen*-style con job? Or does it now face a genuine trademark dispute in a country it's never heard of? Both scenarios are possible. The best answers to this question embraced the factual ambiguity, recommended targeted investigation (the single cleverest thing anyone wrote on this exam was to call the Ruritanian embassy), and suggested appropriate alternative courses of action. It was possible to do well without going down both forks, but it was easier if you did. This was also the question on the exam that called for the most practical judgment. The call of the question explicitly told you to discuss "practical steps" and there were some easy points waiting if you took that suggestion seriously. There was no one best way of organizing an answer. I looked for a combination of appropriate strategy, viable legal theories, and good use of facts.

Goals

Your client, Ultrimpex, has three goals. First, it needs to stanch the bleeding from the loss of its domain name. Recall that a domain name is simply an entry in the DNS databases; when users type that name into their browsers, they're given a particular IP address. They can then use that IP address to request a web site from a server. Ultrimpex still has its IP address, server, and web site content. The only missing link is that customers can't reach any of them by typing "ultrimpex.com" in to their browsers.

Thus, step one has to be registering a new domain name ASAP. (Ultrimpex.biz? Ultrimpex-nyc.com? Ultrimpex.nu?) Once the domain name is up and pointing at Ultrimpex's web site, it should reach out to its clients and inform them of the new URL. Asking search engines to make the switch couldn't hurt, either. The aim is to reduce the number of people who are looking for Ultrimpex and can't find it.

Step two is to start trying to recover control of the ultrimpex.com domain name in the short run. An obvious step—so obvious that most of you missed it—is to try to get in touch with Gazblom. The phone number and the address are no good, but maybe the email address works. Perhaps they're people who can be negotiated with, and perhaps this whole brouhaha is a gigantic misunderstanding. It's a long shot, but it costs you nothing.

You could also work on DomainWheel. Perhaps they can be persuaded to transfer the domain name back, just as they were persuaded to transfer it in the first place. If you can convince them that there's been a mistake, you might also be able to convince them to set it right. Pick up the phone. In the alternative, you could go to court seeking a preliminary injunction ordering DomainWheel to transfer the domain back to you. (You could also seek a TRO preventing them from making any other changes or allowing it to be transferred to another registrar in the interim.)

(Perhaps you may object that suing DomainWheel and asking it nicely don't go well together. Well, that's just an opportunity for strategizing: which do you think is more likely to succeed? Could you try one and then the other? In which order? Could you and the Ultrimpex CEO play good-cop/bad-cop with DomainWheel? Who takes which role? These are the kinds of choices that lawyers need to make all the time; clients will pay you, in part, for making them well.)

Step three is to seek legal relief that gives you permanent control over the domain and compensates you for your losses. Here, Gazblom and DomainWheel are the two most plausible defendants, as all of you understood. TripleClick might have deep pockets, but it's extremely hard to reach them on a trademark cause of action. All they're doing is serving up ads in response to requests; they have no control over the domain *name* that's the heart of the possible infringement. You could go after them on a contributory trademark infringement claim—and I gave a point for working through the *Tiffany* analysis—but in the real world, the courts have rejected such claims.

Suing Gazblom

Your first obstacle here is to convince a U.S. court (it seems unlikely that Ultrimpex could afford foreign litigation) that it has jurisdiction over Gazblom. But that's easy; Gazblom sent an email to a New York domain registrar for the specific purpose of (allegedly) defrauding a New York company of a domain “in” New York. That seems sufficient even under an *ALS Scan* “intent to direct” test, and the email claiming a New York address and phone number could also be the basis for a waiver-of-objection-to-jurisdiction argument. Indeed, it's even remotely possible that the address and phone number are mistakes and Gazblom really has a New York office.

Even if that argument should fail, for purposes of recovering the domain name, the ACPA's *in rem* jurisdiction means that you can sue in New York. (Some of you thought that the ACPA confers *quasi in rem* jurisdiction, which would let you seize any of Gazblom's assets in New York. It doesn't; that kind of *quasi in rem* jurisdiction is unconstitutional. See *Shaffer v. Heitner*, 433 U.S. 186 (1977). You need minimum contacts for any lawsuit; *in rem* jurisdiction usually satisfies them because the property at stake is also the subject matter giving rise to the cause of action.)

You'll also need to track down Gazblom and figure out just who it is you're suing. You've got two leads here. First, DomainWheel dealt with Gazblom via email and through DomainWheel's website. That could give you an IP address, which is enough to start the search. Second, TripleClick presumably has not just an IP address but some payment information. Either way, you'll need to persuade them to help, or obtain a civil subpoena from the court where you file the lawsuit against Gazblom. (If I were you, I'd include some John Doe defendants, to be safe.)

Substantively, the ACPA is the best statute to sue under. (Ordinary trademark infringement and dilution are also legally plausible claims; as we didn't really discuss them in class, I didn't expect you to discuss them on the exam.) Ownership of the mark is more something we worry about in IP than in this course, and obviously the marks are confusingly similar, because they're identical. That leaves bad faith. There are two damning facts here. First, the TripleClick ads suggest that Gazblom isn't doing anything legitimate with the domain name. Second, the bad address and phone number on the transfer request would strongly suggest to a court that Gazblom isn't acting in an aboveboard fashion. Keep in mind that that *if* Gazblom is a real Ruritanian company, it may well have legitimate trademark rights in the ULTRIMPEX trademark.

The UDRP is also quite plausible here, and the relevant standards will be quite similar. The speed and low cost of the UDRP make it a good first choice. Some of you speculated that

Ultrimpex may have been the defendant in a UDRP arbitration it never found out about. That's a clever point, and worth investigating. (It does not mean, however, that you may have only a few days to act. The 10-day deadline is the time that the registrar must wait before transferring the domain to the prevailing complainant; here, DomainWheel has already transferred the domain.)

One last way you might be able to sue Gazblom is under the CFAA. There is an argument that the forged letter or its access to DomainWheel's system constitute access without authorization. Only under the *Shurgard* test is it possible to reach that result, and even there it's questionable. Gazblom never, to your knowledge, accessed the server on which the Ultrimpex web site sat. Thus, Ultrimpex isn't the party whose authorization counts; whereas DomainWheel seems to have consented to everything Gazblom did.

Suing DomainWheel

Kremen v. Cohen provides the roadmap here. Your main lawsuit is for conversion (possibly pleaded as negligence). In making your case that DomainWheel's actions were irresponsible, three facts seem particularly relevant. First, DomainWheel should have notified Ultrimpex of the transfer. This fact is less telling than in *Kremen*, where the transfer order purported to come from the domain owner. But still, Ultrimpex could easily have prevented the problem if it had been notified. Second, acting on the basis of a legal document you're unable to read seems grossly irresponsible. DomainWheel should have, at the very least, translated and authenticated the document. Third, DomainWheel never confirmed any of the contact information it was given—another check that might have led them to suspect that all was not well.

The first potential monkey wrench here is the Ruritanian judgment. You may suspect that it's a forgery, but you don't know that for certain. Even if it's valid, though, you still have a good argument that DomainWheel shouldn't have acted on it. It's not a United States judgment; it's Ruritanian. The U.S. marshals won't kick in DomainWheel's door if it ignores the judgment. Moreover, given that Ultrimpex was never even notified of the Ruritanian action, it seems unlikely that a U.S. court would allow enforcement of the judgment here.

The second issue to tee up is the problem of Ultrimpex's contract with DomainWheel. Perhaps the contract contains express promises by DomainWheel as to its procedures. Perhaps it expressly disclaims liability for negligence in mishandling domains. Either way, you should have a look at the contract, as it will substantially affect possible remedies against DomainWheel. Per *Kremen*, you probably can't claim any rights as a third-party-beneficiary under the DomainWheel-ICANN contract.

Question Sources

The question is a *Kremen v. Cohen* variant, albeit one in which matters are a little less black-and-white. Ultrimpex is a compressed version of "Ultra Import/Export," which is a generic (!) enough name that perhaps someone else far away is using it too. Gazblom is meaningless but sounds vaguely Slavic. DomainWheel is just your average irresponsible registrar; *TripleClick* is based on DoubleClick. Ruritania was the name of the Eastern European monarchy that was the setting for Anthony Hope's 1894 novel *The Prisoner Of Zenda*.