A NEW COMMON LAW OF WEB SCRAPING

by
Benjamin L.W. Sobel [*]

The Clearview AI facial recognition scandal is a monumental breach of privacy that arrived at a particularly inopportune time. A shadowy company reportedly scraped billions of publicly-available images from social media platforms and compiled them into a facial recognition database that it made available to law enforcement and private industry. To make matters worse, the scandal came to light just months after the Ninth Circuit's decision in hiQ v. LinkedIn, which held that scraping the public web probably does not violate the Computer Fraud and Abuse Act (CFAA). Before hiQ, the CFAA would have seemed like the surest route to redress against Clearview. This Article analyzes the implications of the hiQ decision, situates the Clearview outrage in historical context, explains why existing legal remedies give aggrieved plaintiffs little to no recourse, and proposes a narrow tort to empower ordinary Internet users to take action against gross breaches of privacy by actors like Clearview: the tort of bad faith breach of terms of service.

Section II argues that the Ninth Circuit's hiQ decision marks, at least for the time being, the reascension of common law causes of action in a field that had been dominated by the CFAA. Section III shows that the tangle of possible common law theories that courts must now adapt to cyberspace resembles the strained property and contract concepts that jurists and privacy plaintiffs reckoned with at the turn of the twentieth century. It suggests that modern courts, following the example some of their predecessors set over a century ago, may properly recognize some common law remedies for present-day misconduct. Section IV catalogs familiar common law claims to argue that no established property, tort, or contract claim fully captures the relational harm that conduct like Clearview's wreaks on individual Internet users. Section V proposes a new tort, bad faith breach of terms of service, that can provide aggrieved plaintiffs

[*] Affiliate, Berkman Klein Center for Internet & Society, Harvard University. I am grateful to Saptarishi Bandopadhyay, Alvaro Bedoya, Dinis Cheian, Gabe Doble, Terry Fisher, John Goldberg, Joe Gratz, James Grimmelmann, Ben Hopper, Spencer Livingstone, Henry Smith, Rebecca Tushnet, and Salomé Viljoen for comments that have clarified and improved my arguments, and to the Harvard Law School Project on the Foundations of Private Law for financial support of this project.

with a proper remedy without sacrificing doctrinal fidelity or theoretical coherence.

I. INTRODUCTION

On January 18, 2020, the investigative journalist Kashmir Hill broke a sensational story: a "secretive" startup, Clearview AI, offers facial recognition software that identifies persons of interest against a database of nearly three billion photographs.[1] The company's CEO initially claimed that the software was "strictly for law enforcement," but later reporting revealed that Clearview's app was also used by private companies to surveil their premises—and even by private individuals to vet dinner dates.[2]

Clearview did not invent facial recognition technology or pioneer a particularly powerful algorithm. Nor did Clearview develop a business model that allowed it to license a singularly comprehensive photo database. Instead, Clearview reportedly just "scraped" publicly-accessible photographs from sites like Facebook, YouTube, Twitter, and Instagram. That is, Clearview harvested images in bulk, using automated software—in violation of the sites' Terms of Service, which prohibited that very activity.[3]

The Clearview *exposé* outraged civil society.[4] Days after Hill's story broke, a

[1] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Hill's report focused on law enforcement applications, but a subsequent leak of Clearview's client list revealed that it also offered its services to private entities. Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[2] Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. TIMES (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html; Mac et al., *supra* note 1.

[3] Hill, *supra* note 1.

[4] *See generally, e.g.*, Jennifer Lynch, *Clearview AI—Yet Another Example of Why We Need a Ban on Law Enforcement Use of Face Recognition Now*, ELECTRONIC FRONTIER FOUND. (Jan. 31, 2020), https://www.eff.org/deeplinks/2020/01/clearview-ai-yet-another-example-why-we-need-ban-law-enforcement-use-face; Ryan Mac et al., *Clearview AI Once Told Cops To "Run Wild" With Its Facial Recognition Tool. It's Now Facing Legal Challenges*, BUZZFEED NEWS (Jan. 28, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-cops-run-wild-facial-recognition-

putative class action was filed against Clearview and its founder, alleging violations of an Illinois biometric privacy statute, violations of constitutional rights related to Clearview's collaboration with law enforcement, and unjust enrichment.[5] Twitter sent Clearview a letter demanding that Clearview desist from scraping Twitter and delete the data it had collected.[6] Senator Ed Markey sent Clearview an inquiry into its partnerships with law enforcement, and a New York state legislator introduced a bill to prohibit police use of facial recognition technology.[7]

The timing of the Clearview revelations seemed particularly inopportune. Just four months earlier, in *hiQ v. LinkedIn*, the Ninth Circuit had held that scraping publicly available information from professional profiles on LinkedIn may not violate the Computer Fraud and Abuse Act (CFAA).[8] The court acknowledged an argument that LinkedIn users might "retain some privacy interests" in the information on their profiles, but affirmed an injunction prohibiting LinkedIn from blocking a startup's data-scraping.[9]

The CFAA would have been the most obvious statute that platforms could have used in a civil action against Clearview—although even under the CFAA, web scraping is a legal enigma.[10] Given the factual similarities between *hiQ* and the Clearview scandal, commentators have observed that the *hiQ* ruling strengthens Clearview's legal position.[11] But even if the CFAA may not prohibit Clearview's alleged conduct, the company is hardly immune from liability. Aware of the vacuum created by its interpretation of the CFAA, the Ninth Circuit enumerated a laundry list of claims that an aggrieved party might still assert against a scraper: "trespass to chattels claims . . . copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy . . . ."[12] The length and breadth

---

lawsuits.

[5] First Amended Class Action Complaint at 19–32, Mutnick v. Clearview AI, Inc., No. 20 C 512, 2020 WL 4676667 (N.D. Ill. Aug. 12, 2020) [hereinafter FAC, *Mutnick*].

[6] Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, N.Y. TIMES (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html.

[7] Letter from Senator Edward J. Markey to Hoan Ton-That, CEO, Clearview AI (Jan. 23, 2020), https://www.markey.senate.gov/imo/media/doc/Clearview%20letter%202020.pdf; S.B. S7572, 2020 Leg., 243rd Sess. (N.Y. 2020).

[8] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 995 (9th Cir. 2019).

[9] *Id.*

[10] Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 377 (2018) ("Most often the legal status of scraping is characterized as something just shy of unknowable, or a matter entirely left to the whims of courts, plaintiffs, or prosecutors.").

[11] Ben Kochman, *Embattled Startup Clearview AI on Uncertain Legal Footing*, LAW360 (Feb. 28, 2020), https://www.law360.com/articles/1242123/embattled-startup-clearview-ai-on-uncertain-legal-footing.

[12] *hiQ*, 938 F.3d at 1004.

of this list illustrates the diverse thicket of legal interests that web scraping implicates. It also shows the profound and persistent legal indeterminacy of an activity that has been commonplace for years.[13]

But treating the Clearview episode as just a test of the CFAA (and the common law theories that might replace it) obscures something more fundamentally bizarre about the controversy. Despite widespread perceptions that Clearview's undertakings have harmed individual Internet users, most of those users have no surefire cause of action against Clearview itself.[14] Rather, the CFAA, and the more plausible claims the Ninth Circuit suggests might replace it, give a right of action to *platforms*, not to their users. Aggrieved users would sit on the sidelines as platforms sue Clearview under the CFAA or related common law claims.[15] Without legislative intervention, it seems like users must delegate the enforcement of their interests to major platforms—even as against actors who have behaved as outrageously as Clearview allegedly has.

This Article's central claim is that, in limited circumstances, users are not powerless against actors like Clearview. Instead, it proposes that courts recognize a narrow claim that users of targeted platforms could assert against Clearview: the tort of bad faith breach of terms of service. Such a claim helps redress the misalignment of incentives between dominant platforms and the users who currently depend on them to police third parties' harmful violations of their terms. In addition to having functional appeal, the cause of action is rooted in relevant precedent. Throughout the twentieth century, common law courts have recognized that certain contracts are so pervasive and so significant that they engender duties that extend beyond the parties to a particular legal instrument. And for the same reasons, courts have held that bad faith breaches of certain contracts cause emotional harms for which victims may recover in tort. These same precedential principles justify a narrow, modern tort of bad faith breach of terms of service.

---

[13] *See* Sellars, *supra* note 10, at 372–75 ("Given its utility, the technique has been adopted widely. One company estimates that about a quarter of all current web traffic comes from web scrapers.").

[14] The one clear exception is Illinois's Biometric Information Privacy Act (BIPA), which has been the basis of other class actions and already is the basis for the lawsuit against Clearview. *See infra*, text accompanying notes 172–173. *See generally* Ben Sobel, *Facial Recognition Technology Is Everywhere. It May Not Be Legal.*, WASH. POST (June 11, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/.

[15] LinkedIn's own briefing reveals this point. It argued, "LinkedIn acted legitimately to protect member privacy and to preserve the trust and goodwill of its members . . ." and concluded its brief by observing, "hiQ's data-scraping is 'not only contrary to the interests of individual LinkedIn users, it is contrary to the public interest.'" Appellant's Reply Brief at 14–15, 28, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019) (No. 17-16783) (internal citations omitted).

A historical perspective reveals more than just a powerful doctrinal basis for the tort of bad faith breach of terms of service. It also illuminates the problem the tort would help to solve. History explains why, today, Internet users' privacy interests seem to hinge on competing legal forms from both contract and property law—and it helps predict how today's courts may deploy these concepts. The construction of privacy as a hybrid of personal property interests and implied contracts dates back to the English jurisprudence that Samuel Warren and Louis Brandeis synthesized in *The Right to Privacy*.[16] Repudiations of Warren and Brandeis by turn-of-the-century jurists reveal how these same contract and property doctrines might operate against today's privacy plaintiffs. Finally, examining how courts have interpreted socially-indispensable contracts to create "special relationships" and tort duties to third parties explains the origins of modern-day proposals for "information fiduciaries."[17]

Section II of this Article is expository and predictive. It first explains the uncertain legal status of unauthorized scraping of public information and introduces the myriad legal doctrines that could govern the activity. Next, Section II predicts that the judiciary will embrace common law forms to determine the CFAA's reach and to adjudicate cases that fall beyond it.

Section III situates those common law forms in historical context. It argues that the legal indeterminacy of web scraping resembles the tangle of nineteenth-century contract and property case law that Warren and Brandeis unraveled to reveal a right to privacy.[18] Already, plaintiffs in various jurisdictions have asserted imaginative property and contractual claims against Clearview. These claims, both factually and analytically, parallel the claims that plaintiffs made in turn-of-the-century privacy cases following Warren and Brandeis's distillation of a common law right to privacy. Judicial responses to the vanguard privacy torts of the twentieth century illuminate the proper role of the courts in providing redress for today's privacy concerns, as well as the argumentative strategies that might serve or disserve today's plaintiffs.

Section IV explicates the plausible common law claims that users and platforms might assert against unauthorized scraping. It observes that the law of personal and intellectual property is generally ill-suited to fill the void the waning CFAA has created, at least with respect to scraping publicly-available data. Established relational doctrines better address the problem, but are on their own inadequate: in almost all states, today's law leaves users with no clear recourse.

Section V explains the "trust-your-overlords" problem: the mismatched incentives and capabilities that can prevent platforms from protecting users against third parties' privacy abuses. It discusses proposals for, and criticisms of, an "information

---

[16] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[17] *See infra* Section V.A.1.

[18] *See generally* Warren & Brandeis, *supra* note 16.

fiduciary" system to correct these incentives. Section V observes that jurists focused on regulating platforms' terms of service can take lessons from the common law's responses to other pervasive and consequential contracts. The California Supreme Court has read contracts for socially significant services to give rise to duties to nonparties. The court has also recognized that the importance of certain contracts in modern life makes it appropriate to award tortious damages against parties who breach them intentionally and in bad faith. Section V synthesizes these two principles to derive a new cause of action: the tort of bad faith breach of terms of service. The tort permits users in privity with an Internet platform to recover against a third party that is also in privity with the platform, when that third party willfully breaches a material covenant in the terms of service, with knowledge or reckless disregard that its actions will harm the plaintiff. The new cause of action will not singlehandedly fix the discontents of networked capitalism. But a novel common law tort is far easier to implement than the more comprehensive solutions that other scholars and commentators have proposed, and could provide relief while sweeping changes elude us.

II. CYBERLAW'S COMMON LAW TURN

In September 2019, the Ninth Circuit issued its latest major interpretation of the Computer Fraud and Abuse Act.[19] *hiQ Labs, Inc. v. LinkedIn Corp.* considered whether the professional networking website LinkedIn could invoke the CFAA against hiQ, a data analytics company that automatically collected and copied ("scraped") information that LinkedIn's users had uploaded to their public profiles.[20] The Ninth Circuit concluded that hiQ raised a serious question as to whether its conduct was proscribed by the CFAA.[21] The day of the decision, one of the foremost computer trespass scholars called it a "hugely important" development in CFAA jurisprudence.[22]

hiQ's digestible takeaway is that scraping a publicly-available website does not violate the CFAA, even if the site's terms of service prohibit that scraping. This legal proposition may be the case's practical significance. However, *hiQ*'s precise holding contains several qualifications. The case's idiosyncratic, convoluted posture—an appeal from a district court's grant of a preliminary injunction, reviewing the likelihood that the CFAA preempts a state law tortious interference claim[23]—differentiates it from a final judgment on the merits. The Ninth Circuit is just one appellate

[19] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019).

[20] *Id.* at 991.

[21] *Id.* at 1001.

[22] Orin S. Kerr, *Scraping A Public Website Doesn't Violate the CFAA, Ninth Circuit (Mostly) Holds*, VOLOKH CONSPIRACY (Sept. 9, 2019), https://reason.com/2019/09/09/scraping-a-public-website-doesnt-violate-the-cfaa-ninth-circuit-mostly-holds/.

[23] *See hiQ*, 938 F.3d at 999.

jurisdiction, albeit a leader on cyberlaw issues. And finally, LinkedIn has petitioned the Supreme Court to review the Ninth Circuit's decision, and hiQ has responded at the Court's request.[24]

Qualifications notwithstanding, this Section accepts that *hiQ* effectively held that scraping publicly-available information does not violate the CFAA. Such an interpretation of the CFAA represents a return to an earlier era of cyberlaw jurisprudence that favored common law causes of action. In fact, the Ninth Circuit enumerated these causes of action to illustrate that "entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply: state law trespass to chattels . . . copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy" claims may all be available.[25] This Section traces the history of cybertrespass actions—from common law to an expansive CFAA and back again—and predicts a renewed invigoration of under-theorized common law concepts.

A. Cyberlaw's Common Law Origins

The earliest cases in the "cybertrespass" genre resuscitated old common law causes of action, like trespass to chattels. A claim for trespass to chattels, also known as trespass to personal property, can have several formulations. As applied to electronic trespasses to computer servers, the following is most pertinent: a tortfeasor is liable for trespass to chattels if she "us[es] or intermeddl[es] with a chattel in the possession of another" *and* her use impairs the chattel "as to its condition, quality, or value."[26] The high-water mark of trespass to chattels remains *eBay v. Bidder's Edge*, a 2000 case in which eBay sued an auction aggregator site for "crawling" eBay's site in order to copy and display information about eBay's auctions. Even though Bidder's Edge's crawlers consumed a negligible amount of eBay's server bandwidth, a federal district court found eBay likely to succeed on its California state-law trespass to chattels claim.[27] The court reasoned that denying injunctive relief to eBay would invite unrestricted crawling of its site, and the aggregate effect of these negative interferences could substantially impair eBay's computer systems.[28] Notably, eBay also asserted a claim under the CFAA, but the court did not rule on it.[29]

Early scholarly responses to cybertrespass cases like *Bidder's Edge* often argued that real and personal property were poor analogues to cyberspace, and that early

---

[24] Petition for Writ of Certiorari, LinkedIn Corp. v. hiQ Labs, Inc., No. 19-1116 (U.S. Mar. 9, 2020); Brief in Opposition, LinkedIn Corp. v. hiQ Labs, Inc., No. 19-1116 (U.S. June 25, 2020).

[25] *hiQ*, 938 F.3d at 1004.

[26] RESTATEMENT (SECOND) OF TORTS §§ 217, 218 (1965) (AM. L. INST. 1964).

[27] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071–72 (N.D. Cal. 2000).

[28] *Id.*

[29] *Id.* at 1069.

decisions gave website proprietors overbroad rights.[30] In 2003's *Intel v. Hamidi*, the California Supreme Court disavowed the broadest interpretation of *Bidder's Edge*. *Hamidi* held that a state trespass to chattels claim requires "actual or threatened injury to the personal property or to the possessor's legally protected interest in the personal property."[31] The case considered whether a former Intel employee had trespassed upon Intel's servers by sending unsolicited mass mailings to Intel employees who used company email accounts.[32] The Court clarified that *eBay v. Bidder's Edge* cannot be interpreted to state that California law treats even *de minimis* uses of others' bandwidth as trespass to chattels.[33] Because Intel had not demonstrated that Hamidi's emails caused "some measurable loss from the use of its computer system," the record did not support summary judgment in Intel's favor.[34] *Hamidi*'s holding diminished the viability of trespass to chattels claims and may have inspired greater reliance on CFAA claims.

At the same time as they asserted trespass to chattels claims, websites also brought breach of contract actions against defendants who used automated technologies to crawl their sites.[35] At least some of these contract claims were held to raise triable issues.[36] Other cases dismissed breach of contract suits predicated on terms of service on the grounds that "browsewrap" terms did not create enforceable contracts.[37]

Both breach of contract and trespass to chattels claims appear in contemporary cybertrespass complaints as well.[38] At least until *hiQ*, however, common law claims were often subordinated to the CFAA in actual litigation. In *hiQ*, for example, LinkedIn asserted trespass to chattels and misappropriation claims, but the Ninth Circuit limited its analysis to the CFAA because LinkedIn "chose[] . . . to focus on

---

[30] *See generally* Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421 (2002); Michael A. Carrier & Greg Lastowka, *Against Cyberproperty*, 22 BERKELEY TECH. L.J. 1485 (2007).

[31] Intel Corp. v. Hamidi, 71 P.3d 296, 311 (Cal. 2003).

[32] *Id.* at 301.

[33] *Id.* at 305–06.

[34] *Id.* at 306–07.

[35] *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248, 251–52 (S.D.N.Y. 2000) (finding likelihood of success on breach of contract claim, trespass to chattels claim, and CFAA claim, and finding injunction warranted for breach of contract), *aff'd as modified*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 432 (2d Cir. 2004) (Leval, J.) (finding that plaintiff was not likely to succeed on breach-of-contract claim, and that a grant of an injunction based on irreparable harm constituted clear error).

[36] *See, e.g.*, Ticketmaster Corp. v. Tickets.Com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *1 (C.D. Cal. Mar. 7, 2003).

[37] Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 937 (E.D. Va. 2010).

[38] *See, e.g.*, DHI Grp., Inc. v. Kent, No. H-16-1670, 2017 WL 8794877, at *4–7 (S.D. Tex. Apr. 21, 2017) (examining trespass to chattels, CFAA, and breach of contract claims).

a defense based on the CFAA . . . ."[39] As the CFAA developed into the foremost cybertrespass law, common law claims took on a more marginal role.

B. The Burgeoning CFAA

As the *hiQ* litigation suggests, somewhere between *Bidder's Edge* and *hiQ*, the CFAA displaced common law claims as the premier cybertrespass cause of action. In pertinent part, the CFAA criminalizes "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer."[40] The CFAA also contains a civil provision that permits "[a]ny person who suffers damage or loss by reason of a violation of this section" to maintain a civil action.[41] By its terms, this private right of action does not extend to every nominal CFAA violation, but its limitations—such as a minimum of $5,000 in damages—are typically easy to satisfy.[42]

The CFAA's prominence can be explained by the advantages it can offer over coterminous state-law claims. It is a federal statute, so it gives rise to federal question jurisdiction in situations where plaintiffs might otherwise be confined to state court.[43] CFAA claims may permit recovery for substantially the same conduct as trade secret claims, without requiring plaintiffs to demonstrate that any misappropriated information is protectable as trade secrets, nor that it was protected by reasonable measures.[44] After several high-profile, draconian criminal prosecutions, the statute gained a place in the popular imagination as "the most hated law on the internet."[45] The CFAA fused stiff penalties to civil offenses: as Lawrence Lessig put it in a pithy online comment, the CFAA made it "a felony to breach a contract."[46]

Andrew Sellars has cataloged three phases of CFAA jurisprudence. In the first, courts interpreted the CFAA expansively, and found violations when plaintiffs could

---

[39] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 995 (9th Cir. 2019).

[40] 18 U.S.C. § 1030(a)(2)(C) (2018).

[41] § 1030(g).

[42] Sellars, *supra* note 10, at 376.

[43] 28 U.S.C. § 1331 (2018); *see also* Shawn E. Tuma, "*What Does CFAA Mean and Why Should I Care?*"*—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 160 (2011).

[44] Audra Dial & Daniel G. Schulof, *The Computer Fraud and Abuse Act: An Underutilized Litigation Weapon*, KILPATRICK TOWNSEND, https://www.kilpatricktownsend.com/~/media/Files/articles/ADial%20DSchulof%20Technology%20Litigation%20Desk%20Reference_The%20Computer%20Fraud%20and%20Abuse%20Act.ashx (last visited Jan. 27, 2021).

[45] Grant Burningham, *The Most Hated Law on the Internet and Its Many Problems*, NEWSWEEK (Apr. 16, 2016), https://www.newsweek.com/most-hated-law-internet-and-its-many-problems-cfaa-448567.

[46] Lawrence Lessig (@lessig), REDDIT (Jan. 15, 2013, 8:25 PM), https://www.reddit.com/r/technology/comments/16njr9/im_rep_zoe_lofgren_im_introducing_aarons_law_to/c7xmx6j/.

show that a scraper violated either a technical or a contractual prohibition on access.[47] In the second, courts began to narrow the CFAA by differentiating between restrictions on *access to* information and restrictions on *use of* accessible information, and permitting CFAA actions to enforce the former but not the latter.[48] Generally speaking, access restrictions are technical measures that limit access to authenticated users.[49] Use restrictions are terms that restrict how otherwise accessible data may or may not be used.[50] Finally, Sellars suggests a third phase of CFAA caselaw, in which courts have expanded the statute somewhat to include cases in which a website has revoked access to a particular party in order to enforce a use restriction.[51] This revocation would typically take the form of a cease-and-desist letter.[52] *hiQ* marks a departure from the revocation theory.

C. The Waning CFAA (and the Waxing Common Law?)

The Ninth Circuit's *hiQ* decision, issued after Sellars published his CFAA survey, seems to narrow the CFAA's "revocation" theory. LinkedIn had issued hiQ a cease-and-desist letter, but that fact alone did not entail that hiQ's subsequent access was "without authorization," because the data hiQ scraped remained publicly accessible to anyone browsing the web.[53] *hiQ* narrows the CFAA's scope within the Ninth Circuit and may widen the split between circuits' interpretations of the CFAA.[54]

The Supreme Court may soon clarify some issues of CFAA interpretation in *Van Buren v. United States*, a police officer's appeal of a CFAA conviction for using a police database for improper purposes.[55] *hiQ* and *Van Buren* are not identical. Factually, *hiQ* concerns access to generally available information for proscribed purposes, while *Van Buren* concerns an authorized individual's use of a private database for an improper purpose. Legally, *Van Buren* depends on the scope of the CFAA's

---

[47] Sellars, *supra* note 10, at 379.

[48] *Id.*

[49] *Id.* at 379–80.

[50] *Id.* at 379.

[51] *Id.* at 380.

[52] *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999 (9th Cir. 2019) ("The pivotal CFAA question here is whether once hiQ received LinkedIn's cease-and-desist letter, any further scraping and use of LinkedIn's data was 'without authorization' within the meaning of the CFAA and thus a violation of the statute.").

[53] *Id.* at 1002.

[54] *See* Sandvig v. Sessions, 315 F. Supp. 3d 1, 22 n.9 (D.D.C. 2018) (listing cases).

[55] *See* United States v. Van Buren, 940 F.3d 1192, 1208 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667 (2020).

prohibition on "exceed[ing] authorized access," while *hiQ* focuses on the prohibition against "access[ing] a computer without authorization . . . ."[56] The Supreme Court may take *Van Buren* as its opportunity to resolve the cybertrespass issues that *hiQ* presents; it may grant certiorari in *hiQ*; or it may wait for another vehicle entirely. If and when the Court does consider the issues *hiQ* presents, there is reason to think that its resolution will reassert the importance of traditional common law forms.

There is reason to anticipate formalistic developments in cybertrespass jurisprudence because the Supreme Court has begun to center its jurisprudence around formal property categories in various subject matter areas. For example, Justice Gorsuch's dissent in *Carpenter v. United States*, a 2018 decision about government searches of cell phone records, advocated a return to a Fourth Amendment jurisprudence predicated on property interests rather than on reasonable expectations of privacy.[57] An even more recent Supreme Court case, *Manhattan Community Access Corporation v. Halleck*, held that a private entity was not a state actor when it operated public access television channels, based in part on the majority's assertion that the channels were purely private property.[58] By contrast, just two years before *Halleck*, a majority opinion by Justice Kennedy had intimated a more functional conception of the First Amendment's operation online when it suggested that using privately-owned social media sites amounted to "speaking and listening in the modern public square."[59]

Halleck extensively cited Justice Thomas's concurrence in a 1996 case, which predicated a First Amendment public-forum analysis on property interests.[60] Indeed, the *Halleck* majority's basis for rejecting an argument that the public access channels were a public forum was that "the City does not possess a formal easement

---

[56] *See id.* at 1205, 1207; hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1108 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019) ("The key question regarding the applicability of the CFAA in this case is whether, by continuing to access public LinkedIn profiles after LinkedIn has explicitly revoked permission to do so, hiQ has 'accesse[d] a computer without authorization' within the meaning of the CFAA.").

[57] Carpenter v. United States, 138 S. Ct. 2206, 2267–68 (2018) (Gorsuch, J., dissenting) ("[T]he traditional approach [in Fourth Amendment jurisprudence] asked if a house, paper or effect was *yours* under law."); *see also* Florida v. Jardines, 569 U.S. 1, 11 (2013) ("One virtue of the Fourth Amendment's property-rights baseline is that it keeps easy cases easy.").

[58] Manhattan Cmty. Access Corp. v. Halleck, 139 S. Ct. 1921, 1933–34 (2019). *But see id.* at 1941 (Sotomayor, J., dissenting) ("The key question, rather, is whether the channels themselves are purely private property.").

[59] Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017).

[60] Denver Area Educ. Telecomm. Consortium, Inc. v. F.C.C., 518 U.S. 727, 828 (1996) (Thomas, J., concurring) ("Our public forum cases have involved property in which the government has held at least some formal easement or other property interest permitting the government to treat the property as its own in designating the property as a public forum.").

or other property interest in those channels."[61] In response, a commentator observed that the decision reasserts the primacy of property analysis in cyberlaw jurisprudence: "*Halleck* could support a new property-based orientation to the state action requirement of forum analysis . . . . Because the Internet property analysis is so awkward, lower courts have avoided it—a practice that *Halleck* throws into question."[62]

This Article cannot anticipate whether, when, and how the Supreme Court will interpret the CFAA. But the preceding paragraphs provide good reason to believe that the Court's interpretation will rely on formal concepts from the common law—concepts that jurists have for decades avoided transposing to the Internet. If it is likely that the justices will rely on common law forms to articulate cybertrespass law, then scholars should provide the justices with the most appropriate formal reasoning. Section III likens the current moment to the turn of the twentieth century, when courts struggled to bend property and contract doctrines to protect privacy interests. Common law jurists can learn from the successes and failures of privacy's nascence in order to offer plaintiffs principled and effective relief in the present day.

III. WARREN AND BRANDEIS ALL OVER AGAIN: WHY COMMON LAW CAN AND SHOULD HELP US

When Abigail Roberson discovered that her photograph had been used in approximately 25,000 advertisements for a flour company without her consent, it sent her into nervous shock.[63] So she sued the flour company on a tort claim unprecedented in New York common law: a theory propounded ten years earlier by Warren and Brandeis called the right to privacy.[64] State trial and appellate courts held that Ms. Roberson stated a claim,[65] but in 1902, the New York Court of Appeals reversed the judgments below.[66] In "starkly formalist" reasoning, the Court rejected the right to privacy set forth in "a clever article in the *Harvard Law Review*."[67]

Warren and Brandeis's article had distilled a right to privacy by synthesizing two lines of jurisprudence that nineteenth-century English jurists invoked to protect privacy interests: property and contract law. The first line of decisions protected information on the grounds that its disclosure originated in an interference with a property right. The second category enjoined offensive disclosures because they arose from a breach of express or implied contracts. Warren and Brandeis repudiated

---

[61] *Halleck*, 139 S. Ct. at 1933.

[62] Manhattan Community Access Corp. v. Halleck, 133 HARV. L. REV. 282, 288–89 (2019).

[63] Roberson v. Rochester Folding Box Co., 64 N.E. 442, 442 (N.Y. 1902).

[64] Roberson v. Rochester Folding Box Co., 71 N.Y.S. 876, 877–78 (App. Div. 1901); Warren & Brandeis, *supra* note 16, at 213.

[65] Warren & Brandeis, *supra* note 16, at 883–84.

[66] *Roberson*, 64 N.E. at 448.

[67] *Id.* at 444; Jared A. Wilkerson, *Battle for the Disclosure Tort*, 49 CAL. W. L. REV. 231, 243 (2012).

the formal distinction: in both lines of jurisprudence, what courts were *really* protecting was a privacy interest.[68] But even as Warren and Brandeis endeavored to synthesize a new cause of action from existing legal forms, some courts resisted privacy plaintiffs' claims for relief.

This Section observes that the thicket of common law that Warren and Brandeis surveyed resembles the thicket of property and relational claims that web scraping might engender today. In fact, aggrieved Internet users have already begun to assert tenuous common law claims against Clearview. These plaintiffs' complaints invoke both property theories and quasi-contractual theories and, perhaps inadvertently, illustrate the shortcomings of either framework asserted alone. This Section glosses the history of both the property and the contractual approaches to asserting privacy claims and explains the ways in which recent Clearview-related pleadings draw on both approaches. Finally, it concludes that common law courts' responses to *The Right to Privacy* illustrate how courts should, and should not, respond to plaintiffs who seek redress against Clearview.

A. Privacy From Property

In the late 1800s—and arguably today—property doctrine remained the most intuitively appealing mechanism for asserting privacy interests. The jurisprudence that Warren and Brandeis surveyed oscillated between *in rem* claims deriving from the misappropriation of a particular manuscript or print, and common law intellectual property claims that reserved to an author the right of first publication of information he authored.[69] Warren and Brandeis invoke *Prince Albert v. Strange*, a case that enjoined the publication of a catalog describing etchings created by Prince Albert.[70] The defendants in the case apparently had obtained copies of the etchings surreptitiously, without the Prince's consent.[71] The presiding chancellor emphasized the plaintiffs' "entitle[ment] to decide whether, and when, and how, and for whose advantage, their property shall be made use of" and held that the defendant's publication "affects such property as to entitle the Plaintiff to the preventive remedy of an injunction."[72] Warren and Brandeis observed that *Prince Albert v. Strange*

---

[68] Warren & Brandeis, *supra* note 16, at 205.

[69] *Gee v. Pritchard*, for example, used a property rationale to sustain an injunction against publishing copies of compromising letters that the plaintiff had sent to the defendant. Part of the chancellor's basis for sustaining the injunction in *Gee* was that the defendant had returned the original letters to the plaintiff: when "the Defendant having so much of property in these letters as belongs to the receiver, and of interest in them as possessor, thinks proper to return them to [the author] . . . the defendant, if he previously had it, has renounced the right of publication." Gee v. Pritchard (1818) 36 Eng. Rep. 670, 679 (Ch).

[70] *See* Prince Albert v. Strange (1849) 64 Eng. Rep. 293, 293 (Ch).

[71] *See id.* at 293–94.

[72] *Id.* at 313.

stretched the intellectual property rationale by enjoining not the reproduction of the etchings, but rather the publication of a summary *description* of those etchings.[73] From this holding, Warren and Brandeis extrapolated a solicitude for privacy beyond just the protection of property rights: "Although the courts have asserted that they rested their decisions on the narrow grounds of protection to property, yet there are recognitions of a more liberal doctrine."[74]

Perhaps because biometric information seems like a *res* that should be subject to the dominion of its originator,[75] plaintiffs are already asserting property claims against Clearview. One suit alleges conversion: "Plaintiff['s] . . . biometric identifiers and information, including but not limited to their facial geometries, are identifiable, personal property . . . . Clearview and CDW, without authorization, assumed control over the property . . . ."[76] Tim Wu suggested in a tweet that users should assert intellectual property claims through a "class-action copyright lawsuit" against Clearview.[77] Asserting personal or intellectual property to control factual information extracted, non-rivalrously, from a digital photograph looks a lot like pleading a property interest to enjoin a description of one's etchings or private letters. And finding against Clearview on a conversion or copyright claim would be just as strained as finding for Prince Albert on a property claim.

B. Privacy From Contract

Not all the cases that Warren and Brandeis cited bootstrapped a privacy right from a formal property interest. A second line of precedents vindicated plaintiffs' control over certain forms of information—or information obtained by certain means—by deploying forms from contract law. Representative of this line of precedent is *Abernethy v. Hutchinson*, an 1825 chancery case. *Abernethy* enjoined a medical journal from publishing lectures that the plaintiff had delivered orally. Importantly, *Abernethy* was not formally a property case: the chancellor refused to determine whether Dr. Abernethy held "a property in sentiments and language . . . not deposited on paper."[78] Instead, the chancellor granted an injunction on the basis of an implied contract between the audience and the lecturer, by which the attendees

---

[73] Warren & Brandeis, *supra* note 16, at 202.

[74] *Id.* at 204.

[75] *See, e.g.*, Moore v. Regents of Univ. of California, 793 P.2d 479, 488–93 (Cal. 1990) (discussing, and rejecting, a plaintiff's claim for conversion against medical researchers who used the plaintiff's excised spleen cells without permission to develop commercial pharmaceuticals).

[76] Complaint at 8, Hall v. Clearview AI, Inc., No. 20-cv-00846 (N.D. Ill. Feb. 5, 2020).

[77] Tim Wu (@superwuster), TWITTER (Jan. 18, 2020, 8:26 AM), https://twitter.com/superwuster/status/1218524978225741824.

[78] Abernethy v. Hutchinson (1825) 47 Eng. Rep. 1313, 1316 (Ch).

implicitly agreed not to publish the lectures for profit.[79] Although he did not determine whether the plaintiff could also assert a breach-of-contract claim against the third-party publisher, the chancellor concluded that the plaintiff could enjoin the publication of the lectures: "if there had been a breach of contract on the part of the pupil who heard these lectures, and if the pupil could not publish for profit, to do so would certainly be what this Court would call a fraud in a third party."[80]

An 1831 case, *Murray v. Heath*, further clarifies the distinction between invasions of a property interest and breaches of contract.[81] Murray hired Heath to engrave plates depicting Murray's drawings, which Heath created.[82] Before returning the plates to Murray, Heath made impressions using the plates and kept some of the proofs for himself. The plaintiff sued under a copyright statute and for common law trover.[83] *Murray* held that the defendant had not violated statutory piracy prohibitions because the engraving itself was authorized.[84] Further, the court dismissed the plaintiff's trover action, on the grounds that the proofs in question were the property of the defendant, not the plaintiff.[85] Instead of these statutory or common law property actions, the lords of the King's Bench suggested in dicta that the proper cause of action would have been breach of contract.[86]

Finally, in 1888, the English chancery court decided *Pollard v. Photographic Company*, a case that bears some resemblance to the facts of the Clearview fracas well over one hundred years later. *Pollard* concerned a photographer who displayed and sold an unauthorized reproduction of a photograph of the plaintiff, which the plaintiff herself had commissioned.[87] As in *Abernethy*, property interests were not the basis for the chancellor's decision. Unlike the present-day American rule that grants copyright to photographers by default,[88] a contemporary English statute provided that copyright in a photographic portrait vested in the person who commissioned it.[89] While the *Pollard* plaintiffs had a statutory entitlement to copyright in the photograph at issue, they had not registered that copyright and the defendant's conduct was therefore out of the Act's scope.[90] Accordingly, the chancellor enjoined

---

[79] *Id.* at 1318.

[80] *Id.*

[81] Murray v. Heath (1831) 109 Eng. Rep. 984, 986 (KB).

[82] *Id.* at 985.

[83] *Id.* at 985–86, 988.

[84] *Id.* at 988.

[85] *Id.*

[86] *Id.*

[87] Pollard v. Photographic Co. (1888) 40 Ch D 345, 345 (Ch).

[88] *See, e.g.*, Mannion v. Coors Brewing Co., 377 F. Supp. 2d 444, 454–55 (S.D.N.Y. 2005) (discussing photographers' copyright interests in photographs).

[89] Fine Arts Copyright Act 1862, 25 & 26 Vict. c. 68.

[90] *Pollard*, 40 Ch D at 346.

the photographer on the grounds that his conduct breached an implied term in his contract with Pollard.[91]

Pollard distinguished between the "protection against the world in general" that a statutory copyright would have afforded the plaintiffs and their common law right of action against the defendant for his "breach of contract and breach of faith."[92] The year before *Pollard*, a law court had come to substantially the same conclusion in *Tuck v. Priester*. *Tuck* granted an injunction against a defendant who had made unauthorized reproductions of a watercolor that the plaintiffs had contracted with him to print. "Whether the plaintiffs had any copyright or not," the defendant committed a "gross breach of contract and a gross breach of faith" that left him liable for an injunction.[93] As with the property cases, Warren and Brandeis take a realist reading of the contractual line of precedent: "This process of implying a term in a contract . . . is nothing more nor less than a judicial declaration that public morality, private justice, and general convenience demand the recognition of such a rule, and that the publication under similar circumstances would be considered an intolerable abuse."[94]

Unsurprisingly, plaintiffs have also deployed contractual theories in suits against Clearview. One complaint alleges that Clearview "knowingly and illicitly interfered in Plaintiff's . . . contracts with the platforms and websites to which they entrusted their photographs."[95] Several others assert quasi-contract claims for Clearview's unjust enrichment at users' expense.[96] These claims better reflect the nature of the plaintiffs' grievances. Clearview did not act wrongfully by appropriating proprietary information subject to a generalized right to exclude. Rather, it committed a *relational* breach of faith by violating terms of service and social norms common to all parties to collect users' biometric data without consent.

C. What Common Law Courts Can Do

When New York's highest court decided Abigail Roberson's privacy suit, the majority reasserted the rigid legal forms that Warren and Brandeis had sought to synthesize. The court held fast to the maxim that equity does not protect dignitary injuries with no connection to a property or contract interest.[97] It declined to rec-

---

[91] *Id.* at 351.

[92] *Id.* at 353.

[93] Tuck & Sons v. Priester (1887) 19 QBD 629 (QB).

[94] Warren & Brandeis, *supra* note 16, at 210.

[95] FAC, *Mutnick*, *supra* note 5, at 22.

[96] Complaint at 26, Burke v. Clearview AI, Inc., No. 20-cv-00370-BAS-MSB (S.D. Cal. Feb. 27, 2020); Complaint at 15–16, Broccolino v. Clearview AI, Inc., No. 20-cv-02222 (S.D.N.Y. Mar. 13, 2020).

[97] Roberson v. Rochester Folding Box Co., 64 N.E. 442, 444 (N.Y. 1902).

ognize a freestanding right to privacy that would have afforded Ms. Roberson injunctive relief for the unauthorized use of her likeness.[98]

The *Roberson* opinion tracked a rebuttal to Warren and Brandeis's famous article that Herbert Hadley published in 1895. In it, Hadley distinguished the cases that Warren and Brandeis cited. On Hadley's reading of precedents like *Prince Albert* and *Pollard*, "[t]he word privacy, as used in those decisions, is always in connection with property and it is the 'privacy of property,' not the right to privacy, which equity protects."[99] Following Hadley, the New York Court of Appeals seized on the same forms—indeed, the very same cases—that Warren and Brandeis documented. The court took those forms at face value and held that Ms. Roberson failed to satisfy them:

> In not one of these cases . . . was it the basis of the decision that the defendant could be restrained from performing the act he was doing or threatening to do on the ground that the feelings of the plaintiff would be thereby injured; but, on the contrary, each decision was rested either upon the ground of breach of trust, or that plaintiff had a property right . . . which the court could protect.[100]

The *Roberson* decision was controversial.[101] The New York state legislature reacted to the court's denial of common law privacy rights by establishing a statutory privacy right in 1909.[102] In this respect, *Roberson* seems to represent a vibrant political process. A court prudently refrained from common law activism, and a legislature responded to the resulting public outcry.

Just as easily, however, *Roberson* can stand for baleful judicial narrow-mindedness. Three years after *Roberson*, faced with similar facts, the Georgia Supreme Court recognized a common law right to privacy. Of the justices in the *Roberson* majority, the Georgia Supreme Court wrote:

> [W]e think the conclusion reached by them was the result of an unconscious yielding to the feeling of conservatism which naturally arises in the mind of a judge who faces a proposition which is novel. The valuable influence upon society and upon the welfare of the public of the conservatism of the lawyer, whether at the bar or upon the bench, cannot be overestimated; but this conservatism should not go to the extent of refusing to recognize a right which

---

[98] *Id.*

[99] Herbert Spencer Hadley, *Right to Privacy*, 3 N.W. L. REV. 1, 11 (1895).

[100] *Roberson*, 64 N.E. at 445.

[101] A contemporary letter to the editor of the *New York Times* observed that the *Roberson* case must have made "Lord Coke . . . turn in his grave." A Country Lawyer, *Publishing a Woman's Picture*, N.Y. TIMES, July 13, 1902, at 8.

[102] N.Y. CIV. RIGHTS LAW § 50 (McKinney 1909); *see also* Lohan v. Take-Two Interactive Software, Inc., 31 N.E.3d 111, 119 (N.Y. 2018) (describing the statute as a "response" to *Roberson*).

> the instincts of nature prove to exist, and which nothing in judicial decision, legal history, or writings upon the law can be called to demonstrate its non-existence as a legal right.[103]

Instead of clinging to the "strain[ed]" formalism that earlier courts cited when they "really protected the right of privacy"—and which sunk Roberson's case—the Georgia Supreme Court recognized the right to privacy that the New York Court of Appeals had rejected.[104]

Like Abigail Roberson, enterprising Internet users are already asserting untested legal claims against Clearview. And just like Warren and Brandeis's article, these plaintiffs' complaints have blended creative property and contract theories in an attempt to assert novel rights in their facial recognition information. As pleaded, these imaginative claims against Clearview stand little chance of surviving a motion to dismiss. If we take *Roberson* as a story of well-functioning governance, and we trust our government to function just as effectively today, this seems like exactly the right outcome. In dismissing these claims, a court might note the popular opprobrium Clearview's alleged conduct has attracted and implore the legislature to intervene to give deserving plaintiffs redress.[105]

But present-day governance may not resemble the *Roberson* era. It is unlikely that a modern-day federal or state legislature would respond so nimbly to redress a privacy outrage, and unlikelier still that a legislative response would afford a private right of action arising out of a novel privacy interest. As one commentator has noted, "the big platforms . . . have just been scared off [from offering facial recognition services] by the toxification of facial recognition," rather than through legislative moratoria.[106] Just four state legislatures have passed laws that might regulate the technology specifically.[107] Of those states, Illinois is the only one that affords a colorable private right of action for nonconsensual collection and use of facial recognition data.[108]

So, if the *Roberson* court knew that its legislature would not redress the harms Roberson alleged, what could it have done to recognize Roberson's claim without

---

[103] Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68, 78 (Ga. 1905).

[104] *Id.*

[105] *See Roberson*, 64 N.E. at 443 ("The legislative body could very well interfere and arbitrarily provide that no one should be permitted for his own selfish purpose to use the picture or the name of another for advertising purposes without his consent. . . . The courts, however, being without authority to legislate, are required to decide cases upon principle, and so are necessarily embarrassed by precedents created by an extreme, and therefore unjustifiable, application of an old principle.").

[106] Stewart Baker, *The Cyberlaw Podcast: Will the First Amendment Kill Free Speech in America?*, LAWFARE (Mar. 5, 2020, 5:05 PM), https://www.lawfareblog.com/cyberlaw-podcast-will-first-amendment-kill-free-speech-america.

[107] *See infra*, Section IV.C.1 (discussing state biometric privacy statutes).

[108] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1 *et seq.* (2008).

being "embarrassed" by the precedents that bound it?[109] This Article accepts as its premise that a common law court in such a position should have and could have recognized a common law remedy for such a plaintiff. It further accepts as its premise that today's common law courts will find themselves in precisely this position as plaintiffs depicted in Clearview's three billion images begin to petition them for relief. The question that animates this Article, then, is this: what can today's common law jurists do to preserve Internet users' legitimate privacy interests against the backdrop of legislative gridlock? Readers interested only in the answer to that question should skip to Section V, which proposes a narrow tort that users of Internet platforms may assert against third parties that cause them privacy harms by willfully breaching certain covenants in those platforms' terms of service. Readers interested in a thorough examination of the post-*hiQ* common law landscape should proceed to Section IV, which argues that, while neither contract nor property alone are adequate to explain users' grievances against Clearview, a contractual perspective is more descriptively accurate and sounder policy.

D. A Qualified Defense of Formalism

So far, this Article might read like a critique of "formalism." It is not. By "formalism," I refer to juridical reasoning that invokes legal "forms"—that is, well-delineated doctrinal categories, like property, contract, and their associated subspecies.[110] Formal legal reasoning, as I use the term, gives primacy to those forms and may typically condition legal conclusions on their presence or absence.[111] Legal realism, in contrast, disregards formal labels and focuses on the substantive relief

---

[109] *Roberson*, 64 N.E. at 443.

[110] Property has a more intricate and determinate constellation of formal subspecies, in contrast to contract's more "whimsical or fanciful" possibilities. *Cf.* Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The* Numerus Clausus *Principle*, 110 YALE L.J. 1, 3–4 (2000). But a contract is of course a legal form, too, albeit one that is more customizable once it has been instantiated. And, crucially, decisions about *whether an instrument or transaction is of the form of a "contract"* will obviously dictate the rights and duties of the parties to that instrument. When the New York Court of Appeals found that Abigail Roberson possessed neither a contractual right, nor a property right, her claim foundered. And when a chancellor finds a contract—or derives what Roscoe Pound might call a "formal peg"—a privacy-like claim prevails. *See* Roscoe Pound, *Equitable Relief Against Defamation*, 29 HARV. L. REV. 640, 644 (1916) (discussing Gee v. Pritchard (1818) 36 Eng. Rep. 670, 679 (Ch)).

[111] I take this sense of "formalism" to resemble what Roberto Unger calls, "the willingness to work from the institutionally defined materials of a given collective tradition and the claim to speak authoritatively within this tradition, to elaborate it from within in a way that is meant, at least ultimately, to affect the application of state power." Roberto Mangabeira Unger, *The Critical Legal Studies Movement*, 96 HARV. L. REV. 561, 565 (1983). My usage is also consonant with Ernest Weinrib's contention that, to the formalist, juridical relationships "are intelligible by reference to themselves and not solely as the translation into law of an independently desirable political purpose." Ernest J. Weinrib, *Legal Formalism: On the Immanent Rationality of Law*, 97

granted or denied in a particular case. Roscoe Pound gives a quintessentially realist dissection of *Gee*, the English proto-privacy case: "[the chancellor] found a way to . . . protect[] [plaintiff's] right of privacy by securing a right in property which had no value as property and was a *mere formal peg on which to hang the substantial relief*."[112] To realists, formalists might seem benighted, or obstinately missing the forest for the trees. Why insist on formal categories like property and contract when everyone involved surely knows that what is *really* at stake is privacy?

That critique of formalism may be accurate, but it risks discounting the *substantive* value of formal analysis. Legal forms help jurists to discern whether something has gone wrong in a particular case and to provide consistent types of relief. Evaluating whether a legal interest is one of "property" or "contract," or neither, helps clarify the nature of a given dispute. Without legal forms to build upon, realists would struggle to articulate with any precision what a given substantive dispute is "really" about. In other words, legal forms may well be contrived, indeterminate, and historically contingent—but so are legal disputes, and legal forms constitute the substrate on which those disputes unfold. Like it or not, then, legal forms permeate our understanding of legal problems. Analyzing those problems in terms of formal interests thus helps both to illuminate some of their substance, as well as to indicate their judicious resolution.

For all this Section's apparent criticism of formal legal reasoning, the Article's overall methodology is formalist. After all, a paucity of formal analysis is arguably what makes it so difficult to pinpoint which step in the construction or use of a nonconsensual facial recognition database begins to invade a subject's interests. Cataloging the formal legal interests that facial recognition does and does not implicate helps substantiate a theory of the harm it causes, both in doctrinal and practical terms. Section IV will inventory the formal interests at stake in the Clearview dispute, not because such an analysis mechanistically determines the dispute's resolution, but because it *illuminates how to address the dispute legally*—which is what Section V then endeavors to do.

IV. WEB SCRAPING LOOKS MORE LIKE A CONTRACTS PROBLEM THAN A PROPERTY PROBLEM

The remedies for unauthorized scraping of publicly-accessible information might be conceptualized as either rights "against the world" or rights "against [a] particular Defendant," or both.[113] Broadly speaking, the former category comprises

YALE L.J. 949, 957 (1988).

[112] Pound, *supra* note 110, at 644 (emphasis added); *see also supra* text accompanying note 69 (discussing *Gee*).

[113] *See* Int'l News Serv. v. Associated Press, 248 U.S. 215, 236 (1918) (citing Morison v. Moat (1851) 68 Eng. Rep. 492, 500 (Ch)).

property rights, and the latter comprises rights in contract and in tort.[114] This Section argues that the law post-*hiQ* rightly denies users and platforms any generalized, property-style rights to control uses of information that they publish to the open Internet. Instead, it advocates that courts adopt a "relational" or "bilateral" approach to remedies, in cases in which remedies are appropriate.[115]

A. Users' Property Interests

This sub-Section surveys the personal and intellectual property interests that users' interactions with platforms may create or implicate.[116] Although a surprising number of baseline personal property issues in cyberspace remain unresolved, the reported facts of the Clearview incident do not show an invasion even of a plausible personal-property interest. The judiciary has elaborated the rules of digital intellectual property more comprehensively. Indeed, some commentators have suggested that individual users assert intellectual property claims against Clearview for its scraping activities.[117] However, this Section concludes that today's doctrine cannot and should not support property and intellectual property claims by Internet users against Clearview.

1. Users' Personal Property Interests

Whether or not a user "owns" her social media account and associated pages are contested legal questions. A social media account may be the intangible property of the user to whom it belongs, such that interfering with its possession may constitute conversion.[118] A business's social media accounts may be assets for the purposes of bankruptcy.[119] A Facebook page associated with and controlled by a government official may not be purely private property.[120]

Given the potential malleability of personal property doctrine in cyberspace, it is unsurprising that a suit recently filed against Clearview by a Facebook, Instagram, and Venmo user alleges conversion.[121] However, the facts of *hiQ* and the Clearview

---

[114] *See* Henry E. Smith, *Modularity and Morality in the Law of Torts*, 4 J. TORT L. 1, 1 (2011).

[115] *Id.* at 17.

[116] A draft manuscript by Christina Mulligan and James Grimmelmann offers a lucid explanation of property interests in digital information that helped me clarify my analysis in this Section. *See generally* Christina Mulligan & James Grimmelman, *Data is Property* (unpublished manuscript) (on file with author).

[117] Wu, *supra* note 77.

[118] *See, e.g.*, Order on Defendant's Motion to Dismiss at 9, 14, PhoneDog v. Kravitz, No. 11-cv-03474-MEJ (N.D. Cal. Nov. 8, 2011); Farm Journal, Inc. v. Johnson, No. 4:19-CV-00095-SRB, 2019 WL 1795945, at *5–6 (W.D. Mo. Apr. 24, 2019).

[119] *In re* CTLI, LLC, 528 B.R. 359, 366–67 (Bankr. S.D. Tex. 2015).

[120] *See* Davison v. Randall, 912 F.3d 666, 682–83 (4th Cir. 2019).

[121] Complaint at 8, Hall v. Clearview AI, Inc., No. 20-cv-00846 (N.D. Ill. Feb. 5, 2020).

fracas do not implicate plausible personal property claims: scraping does not interfere with the possession or use of any of these inchoate property interests. Scraping's intersection with personal property comes from querying servers and reproducing information, not by interfering with control over or access to tangible or intangible property. Thus, while the platforms have somewhat stronger trespass claims, users aggrieved by Clearview's alleged conduct cannot plausibly allege an interference with a personal property interest.[122]

Conversion is "an intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel."[123] Plaintiffs *can* state claims for conversion when a defendant interferes with rivalrous intangible property, such as domain names.[124] Conversion is also appropriate when the information at issue is not necessarily rivalrous, but the defendant deprives plaintiff of its use, such as by deleting all instantiations of data that the plaintiff controlled.[125]

But the information Clearview allegedly scraped from Facebook is not rivalrous, and the acts of scraping did not interfere with Facebook or its users' control over the instantiations of the information they had uploaded to Facebook. Rather, the scraping duplicated the data in question without interfering with the instantiation that the user placed on a platform's servers. That the users did not lose control over the information in question is fatal to a conversion claim. Moreover, even if the unauthorized copying of a photograph did satisfy the elements of a state-law conversion claim, federal copyright law would preempt that claim.[126] A user's action for trespass to personal property would fail for substantially the same reasons.

2. Users' Copyright Interests

IP claims do not require owners to allege deprivation of *control*; rather, they permit rights holders to assert a right to exclude some unauthorized uses of information. Described so generally, IP seems like it might give users suitable recourse against Clearview or hiQ—especially because the photographs Clearview reproduced are almost certainly copyright-protected. However, in both the LinkedIn and Clearview examples, users lack colorable intellectual property claims.

Copyright seems like a plausible hook for Clearview's liability to users. Scraping photographs nominally reproduces those photographs, which is a *prima facie*

---

[122] For a discussion, and ultimately a rejection, of platforms' plausible personal property claims, *see infra* Section IV.B.1.

[123] RESTATEMENT (SECOND) OF TORTS § 222A (1965) (AM. LAW INST. 1964).

[124] *Cf.* Kremen v. Cohen, 337 F.3d 1024, 1036 (9th Cir. 2003).

[125] Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1278 (N.Y. 2007).

[126] *See, e.g.*, Healthcare Advocates, Inc. v. Harding, 497 F. Supp. 2d 627, 650 (E.D. Pa. 2007) (holding that the Copyright Act of 1976 preempted claims for conversion and trespass to chattels predicated on defendant's reproduction, display, and distribution of archived images of plaintiff's website).

infringement of the exclusive rights of their copyright owners. But a copyright claim would be unavailing both practically and doctrinally. Practically, it is not obvious that the aggrieved party will hold the appropriate copyrights. Copyright in photographs vests, by default, in the photographer.[127] Apart from "selfie" photographs, then, the author of social media photographs will be someone other than the person depicted in the photograph. Thus, in a great many cases, aggrieved users will lack an ownership interest that would allow them to enforce copyright.

Mechanics aside, copyright doctrine itself gives rights holders little recourse against the unauthorized use of photographs to train facial recognition programs. I have argued elsewhere that the incidental reproduction of photographs to train facial recognition algorithms does not implicate any copyright-protected interests.[128] Copyright is an economic right, not a privacy protection.[129] Facial recognition does not require any authorial expression to function: the algorithms learn human features, which are innate facts rather than authored expression, and are therefore uncopyrightable.[130]

Thus, it is possible to scrape photographs in a manner that does not reproduce any copyrighted expression, by taking only the portions of a photograph that depict a person's face.[131] Moreover, even if scraping photographs amounted to *prima facie* infringement, the same fair use defense that allows commercial image search engines to proliferate should also find some AI-related reproductions to be non-infringing.[132] In short, individuals aggrieved by facial recognition object to uses of their *likenesses*, rather than their *expression*. A motivation to protect personal features, rather than authorial expression, would undermine copyright claims against entities that scrape photographs for facial recognition—and appropriately so. But weak copyright claims may be a blessing for prospective plaintiffs: the personal nature of the interests at stake in facial recognition diminishes the chances that copyright law would preempt privacy-related causes of action.[133]

---

[127] *See, e.g.*, Mannion v. Coors Brewing Co., 377 F. Supp. 2d 444, 454–55 (S.D.N.Y. 2005).

[128] Benjamin L.W. Sobel, *Artificial Intelligence's Fair Use Crisis*, 41 COLUM. J.L. & ARTS 45, 67–68 (2017).

[129] *See* Garcia v. Google, Inc., 786 F.3d 733, 745 (9th Cir. 2015).

[130] *Cf.* Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 347 (1991) ("No one may claim originality as to facts. This is because facts do not owe their origin to an act of authorship.") (internal quotations omitted).

[131] Indeed, this is how many photographs appear in popular facial recognition training datasets. *See* Sobel, *supra* note 128, at 68.

[132] *Id.*

[133] *Cf.* Midler v. Ford Motor Co., 849 F.2d 460, 462 (9th Cir. 1988) (holding that the tortious appropriation of a distinctive voice is not preempted by copyright law because, "[a] voice is not copyrightable . . . . What is put forward as protectible here is more personal than any work of authorship."), *accord* Waits v. Frito-Lay, Inc., 978 F.2d 1093, 1100 (9th Cir. 1992), *abrogated on other grounds by* Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118 (2014).

The same considerations that make the human face uncopyrightable also make personal and professional information uncopyrightable.[134] Copyright does not give a LinkedIn user a property interest in her professional history, even if she wrote it herself and controls the page on which it appears. Nor does copyright entitle a user to control facts about when and how she edited her profile, which is the information hiQ collects and analyzes.[135]

LinkedIn's cease-and-desist letter to hiQ also alleged that hiQ was violating the Digital Millennium Copyright Act (DMCA).[136] LinkedIn did not "focus on" any copyright-related claims when it appealed the district court's order. [137] The Ninth Circuit did not rule on any copyright or DMCA issues, but it suggested LinkedIn may possess such claims.[138] In support, the Ninth Circuit cited *Associated Press v. Meltwater Holdings*, which rejected a tech company's fair use defense for scraping copyrighted news articles and reproducing snippets of them to its subscribers, in response to keyword alerts set in advance.[139]

Meltwater's scraping differs from hiQ's and Clearview's. The *Meltwater* court observed that the defendant's business model was to "republish designated segments of text from news articles, without adding any commentary . . . in order to make money directly from the undiluted use of the copyrighted material."[140] Unlike Meltwater, neither hiQ nor Clearview has a business model that centers on *republication* of copyrighted materials. hiQ analyzes behavioral information to predict employees' likelihood of seeking other employment. In other words, hiQ takes in uncopyrightable facts and outputs predictions based on its own analyses of those facts. Clearview operates in much the same way, but the facts that Clearview analyzes may happen to be embedded in copyrighted photographs. Clearview takes in factual information from the photographs it scrapes—the facial geometry portrayed in a photograph, paired with the individual identified in that photograph—and uses that information to predict the identity of people in other photographs.

In short, copyright does not provide users with any generalized right to exclude third parties from reproducing or analyzing the factual information they post on the

---

See also 17 U.S.C. § 301(a) (2018) (providing for the preemption of state-law rights "equivalent to any of the exclusive rights within the general scope of copyright"); *infra* note 164 (discussing a recent federal district court order concerning copyright preemption in *Genius Media Group, Inc., v. Google LLC*, No. 19-CV-7279 (MKB), 2020 WL 5553639 (E.D.N.Y. Aug. 10, 2020)).

[134] *Feist*, 499 U.S. at 347–48.

[135] *See* Ticketmaster Corp. v. Tickets.Com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *4 (C.D. Cal. Mar. 7, 2003).

[136] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 992 (9th Cir. 2019).

[137] *Id.* at 995.

[138] *Id.*

[139] Associated Press v. Meltwater U.S. Holdings, Inc., 931 F. Supp. 2d 537, 543 (S.D.N.Y. 2013).

[140] *Id.* at 552.

Internet. To the extent copyright can restrict scraping, it will cover the scraping of expressive information for market-substituting purposes, as was at issue in *Meltwater*. In contrast, Clearview allegedly scraped factual information in order to create a market that major platforms and their users had expressly endeavored to avoid creating. Copyright is neither doctrinally nor theoretically apt for regulating dignitary injuries arising out of unauthorized web scraping.

3. Users' Publicity Rights

Some scholars have observed that publicity rights might provide individuals with recourse against nonconsensual enrollment in facial recognition databases.[141] Publicity rights are statutory and/or common law rights; California recognizes both a statutory right and a common law claim.[142] The right is often treated by courts and litigants as a species of intellectual property.[143] Some scholars, most notably Jennifer Rothman, have disputed this characterization and argued that the right of publicity is better understood as a privacy interest.[144] For its part, the California Supreme Court has asserted that the label is "pointless," because a right with any basis can be monetized by the individual who holds it.[145]

Whatever the right of publicity's proper classification is, its theory of harm is dissimilar from the privacy harms that Clearview may have wrought. The right focuses on economic, rather than dignitary, injuries: it "protects an individual's right to profit from the commercial value of his or her identity."[146] Moreover, the elements of a right of publicity claim clarify that actionable use must be of a "readily identifiable" individual.[147] This requirement makes sense whether as a protection of the privacy interest Abigail Roberson sought to vindicate after being recognizably depicted on a flour box, or the economic interest of an individual whose recognizable likeness and associated cachet are being used without authorization to draw consumers to products.

But a company that produces facial recognition technology does not exactly invade either of these interests. Indeed, *the whole point of facial recognition technology*

---

[141] *See* Brian D. Wassom, *IP in an Augmented Reality*, 6 LANDSLIDE 8, 12 (2014).

[142] CAL. CIV. CODE § 3344(a) (West 2020); *see* Comedy III Prods., Inc. v. Gary Saderup, Inc., 21 P.3d 797, 799 (Cal. 2001).

[143] *See, e.g.*, *id.* at 804 ("The right of publicity, like copyright, protects a form of intellectual property that society deems to have some social utility."). *See generally* Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 CALIF. L. REV. 125 (1993).

[144] JENNIFER E. ROTHMAN, THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD 182 (2018).

[145] Lugosi v. Universal Pictures, 603 P.2d 425, 428 (Cal. 1979) ("[T]he interest in question is one of 'property'. . . . We agree, however, with Dean Prosser who considers a dispute over this question 'pointless.'").

[146] Ross v. Roberts, 166 Cal. Rptr. 3d 359, 365 (Cal. Ct. App. 2013).

[147] CAL. CIV. CODE § 3344(b) (West 2020).

is to identify individuals who are not readily identifiable. Being enrolled in a facial recognition database does not invade someone's privacy by making "conspicuous display of her likeness, in various public places . . . ."[148] Rather, it enables others to link revealing information to one's voluntary displays of one's likeness—information that would have been inaccessible without the technology. This *is* a privacy harm, but it is a harm substantively dissimilar from the harm Roberson alleged over a century ago.

Nor does facial recognition squarely implicate the economic aspects of the right of publicity, as that right is conventionally understood. Clearview does not use any particular person's established commercial appeal to attract customers. Again, essentially the reverse is true: customers use Clearview to identify people whom they do not recognize. That identification may reasonably cause privacy injuries to the individuals identified, but the injury is unlike the damage a plaintiff suffers either through foregone ad revenue or through the reputational harm provoked by being perceived as a hawker of goods.[149]

In sum, the harm of being nonconsensually enrolled in a commercial facial recognition database resembles neither the privacy interests nor the economic interests that the right of publicity encompasses. Indeed, part of the outrage the Clearview episode generated was probably attributable to the belief that individuals' biometric data were not salable commodities—rather than that Clearview simply refused to pay a suitable price.[150] This mismatch does not delegitimize anyone's grievances. It does, however, make the common law and statutory right of publicity a tenuous means of redress.

B. Platforms' Property Interests

The CFAA is the Internet's "own kind of trespass law that closely resembles its physical-world cousin."[151] It remains a powerful tool to discipline intrusions to computer systems that clearly contravene modern trespass norms, like bypassing an authentication requirement using purloined credentials.[152] However, where information is publicly accessible but subject to access or use restrictions in terms of service, both the *hiQ* decision and Kerr's article suggest that the CFAA should no

---

[148] Roberson v. Rochester Folding Box Co., 64 N.E. 442, 449 (N.Y. 1902) (Gray, J., dissenting).

[149] *See, e.g.*, Waits v. Frito-Lay, Inc., 978 F.2d 1093, 1103–04 (9th Cir. 1992), *abrogated on other grounds by* Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118 (2014) (discussing theories of recovery for both injury to feelings and economic harms under California right of publicity).

[150] *See infra* Section IV.C.3 (discussing unjust enrichment theory).

[151] Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1153 (2016).

[152] *Id.* at 1171.

longer be a viable exclusion mechanism.[153] Nevertheless, both the Ninth Circuit and Kerr's article leave open the possibility that other property-like causes of action might be available to website proprietors.[154] This sub-Section argues that these causes of action, while plausible on other sets of facts, are ill-suited to address the unauthorized web scraping of publicly-accessible information undertaken by hiQ and Clearview.[155]

1. Platforms' Personal Property Interests

The previous sub-Section observed that individual users lack clear personal property claims to assert against scrapers. As the Ninth Circuit recognized, platforms may have more plausible trespass to personal property claims against scrapers.[156] Although these claims will be fact specific, it is probable that many scraping activities will not cause the threshold level of injury sufficient to sustain a platform's trespass suit. Under *Hamidi*, a trespass to personal property plaintiff must "demonstrate some measurable loss from the use of its computer system" that is "substantial," rather than "momentary or theoretical."[157] Nor, under *Hamidi*, can a plaintiff "bootstrap . . . an injury" by citing its expenses made to prevent unauthorized queries.[158] LinkedIn contended at the district court level that hiQ's scraping "erodes the trust that LinkedIn has cultivated with its members, thereby damaging the platform in which LinkedIn has invested fifteen years and billions of dollars."[159] On appeal, however, LinkedIn itself argued that a trespass to chattels claim would be difficult to sustain due to *Hamidi*'s damage requirement: "Demonstrating that any particular data-scraper has impaired the integrity of data or physically harmed LinkedIn's computer systems will be challenging."[160]

Plenty of clear-cut cases remain within the CFAA's reach, even after *hiQ*. Mass-querying a server in order to overwhelm it with requests and knock it offline—called a distributed-denial-of-service (DDoS) attack—is a paradigmatic trespass to personal property claim.[161] Unlike scraping information, the very object of a DDoS

---

[153] *Id.* at 1165–66.

[154] *Id.* at 1149 n.23.

[155] *See* Sandvig v. Barr, 451 F. Supp. 3d 73, 88 (D.D.C. 2020) ("[T]he analogy between real property and the internet is not perfect.").

[156] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1004 (9th Cir. 2019).

[157] Intel Corp. v. Hamidi, 71 P.3d 296, 306–07 (Cal. 2003).

[158] *Id.* at 308.

[159] LinkedIn Corp.'s Opposition to Plaintiff's Motion for a Temp. Restraining Order at 1, hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099 (N.D. Cal. 2017) (No. 17-CV-03301-EMC).

[160] Appellant's Opening Brief at 55, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019) (No. 17-16783).

[161] hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1113 n.11 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019).

attack is to interfere with a server owner's use of her property.

However, simply querying a server in an unauthorized manner rightly does not support a trespass to personal property claim. This obviously does not alter the server's status as the owner's personal property. Accordingly, absent the extraordinary equitable relief granted on *hiQ*'s particular facts, an owner would remain free to implement self-help measures to prevent or mitigate unauthorized queries.

2. Platforms' Intellectual Property Interests

When scraping activities implicate user-uploaded data, as is the case in both the Clearview and *hiQ* scenarios that are this Article's focus, platforms rarely own any intellectual property rights that might subsist in the data in question. Rather, a platform like Facebook or LinkedIn "has only a non-exclusive license to the data shared on its platform, not an ownership interest."[162] Only copyright owners and exclusive licensees may bring copyright suits.[163] Indeed, a recent order from a federal district court indicates that copyright law may in fact *undermine* some anti-scraping suits by preempting relevant state-law claims.[164]

A platform might also attempt to state a claim against a scraper under the anticircumvention provisions of the Digital Millennium Copyright Act, which prohibits circumventing "a technological measure that effectively controls access" to a copyrighted work.[165] Even if a platform had taken some self-help to hinder web scraping of public information, such a claim would be tenuous. As a threshold matter, efforts to mitigate scraping arguably do not "effectively control[] access" if the webpages remain publicly accessible.[166]

Trade secret law may give plaintiffs redress against scrapers who appropriate confidential information, and it may even cover large compilations of publicly-

---

[162] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 998 (9th Cir. 2019).

[163] Granite Music Corp. v. Ctr. St. Smoke House, Inc., 786 F. Supp. 2d 716, 724 (W.D.N.Y. 2011).

[164] *See* Genius Media Grp., Inc., v. Google LLC, No. 19-CV-7279 (MKB), 2020 WL 5553639, at *10, *12, *14 (E.D.N.Y. Aug. 10, 2020). In *Genius*, a lyrics website, Genius, brought breach of contract, unfair competition, and unjust enrichment claims against Google for displaying lyrics that were allegedly scraped from Genius's site without authorization. *Id.* at *1–*2. The plaintiff held licenses to the copyrighted lyrics, but the copyrights remained with music publishers. *Id.* at *1. The court held that "[Genius]'s breach of contract claims are nothing more than claims seeking to enforce the copyright owners' exclusive rights to protection from unauthorized reproduction of the lyrics and are therefore preempted." *Id.* at *16. Potential federal preemption of business torts will be a vital issue as scraping's common-law turn continues.

[165] 17 U.S.C. § 1201(a)(1)(A) (2018). Indeed, LinkedIn's cease-and-desist letter to hiQ included such a claim. *hiQ*, 938 F.3d at 992.

[166] *Cf.* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004) ("[J]ust as one would not say that a lock on any door of a house 'controls access' to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works.").

posted information.[167] Finally, platforms may have viable misappropriation claims.[168] This Article adopts the perspective that misappropriation is better understood as a relational interest, rather than a comprehensive, property-style right to exclude.[169] In fact, misappropriation's relational qualities are what make the cause of action better suited to addressing unauthorized scraping than property remedies.[170] Accordingly, the Article discusses misappropriation in a subsequent relational section.[171]

C. Users' Relational Interests

1. Users' Rights Under State Statutes

The most obvious recourse that individual Internet users may have against Clearview lies in biometric privacy statutes enacted at the state level. Four states have biometric privacy statutes that restrict how firms may process facial recognition data: Illinois, Texas, Washington, and California. California, Texas, and Washington permit the state attorney general to enforce civil penalties against violations.[172] The

---

[167] *See, e.g.*, Compulife Software Inc. v. Newman, 959 F.3d 1288, 1314 (11th Cir. 2020) ("Nor does the fact that the defendants [scraped] [data] from a publicly accessible site automatically mean that the taking was authorized or otherwise proper. Although Compulife has plainly given the world implicit permission to access as many quotes as is *humanly* possible, a robot can collect more quotes than any human practicably could. So, while manually accessing quotes from Compulife's database is unlikely ever to constitute improper means, using a bot to collect an otherwise infeasible amount of data may well be . . . ."); DHI Grp., Inc. v. Kent, 397 F. Supp. 3d 904, 923 (S.D. Tex. 2019) (denying summary judgment to both parties on a trade secret claim arising out of the unauthorized scraping of a resume database); *see also* United States v. Nosal, 844 F.3d 1024, 1042 (9th Cir. 2016) ("[A] trade secret may consist of a compilation of data, public sources or a combination of proprietary and public sources. It is well recognized that it is the secrecy of the claimed trade secret as a whole that is determinative.").

[168] *See, e.g.*, Int'l News Serv. v. Associated Press, 248 U.S. 215, 236 (1918).

[169] *See generally* Shyamkrishna Balganesh, *"Hot News": The Enduring Myth of Property in News*, 111 COLUM. L. REV. 419 (2011).

[170] Misappropriation also incorporates equitable considerations that could thwart opportunistic uses of governing law. *See* Henry E. Smith, *Equitable Intellectual Property: What's Wrong with Misappropriation*, *in* INTELLECTUAL PROPERTY AND THE COMMON LAW 43, 45 (Shyamkrishna Balganesh ed., Cambridge Univ. Press 2013). Equity's *ex post* remedial discretion saves the law from having to foreclose, *ex ante*, every loophole an unscrupulous startup might exploit. *See id.* at 53. At the same time, however, broader judicial discretion to interpret commercial morality—if wielded by a decisionmaker unfamiliar with the norms of Internet enterprise—may disrupt a business ecosystem that, for all its faults, has developed simple and effective technological rules to dictate appropriate behaviors. *Cf. id.* at 43. *See also infra* Section V.B.3 (discussing the robots.txt exclusion standard).

[171] *See infra* Section IV.D.

[172] CAL. CIV. CODE § 1798.155(b) (West 2020), *amended by* 2020 Cal. Legis. Serv. Prop. 24, § 1798.155(b) (West 2020); TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2017); WASH. REV. CODE ANN. § 19.375.030 (2020).

Illinois Biometric Information Privacy Act (BIPA) is the only statute that gives individuals a private right of action.[173] At least one state Attorney General's office, Vermont, has filed a complaint against Clearview using its consumer protection authority.[174]

Perhaps unsurprisingly, the BIPA has given rise to the most involved litigation to date. The Illinois Supreme Court held in 2019 that plaintiffs need not assert a particular injury beyond a violation of their statutory rights to sue under the act.[175] Facebook recently settled a suit brought under the BIPA for $550 million.[176] Companies like Google have made facial recognition-related applications unavailable in Illinois.[177] Illinois plaintiffs are already invoking the BIPA against Clearview.[178]

Biometric privacy statutes, and the BIPA in particular, seem like individual users' best weapon against Clearview, but they have limitations. The first and most obvious limitation is that these laws cover only four states, and of those states, only Illinois affords a private right of action. But the substance of some of the laws may also be less than wholly adequate to address the problem of nonconsensual facial recognition software. The plain text of both the Illinois and Washington statutes, for example, appears to specifically exclude photographs *and information derived from photographs* from their definitions of biometric identifiers.[179]

2. Users' "Privacy Tort" Claims

Previous commentators have observed that the familiar privacy torts, most famously elaborated by Prosser, "are simply too antiquated to handle th[e] unique problem" of facial recognition.[180] Prosser identified four privacy torts: "intrusion

---

[173] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/20 (2008).

[174] *See generally* State of Vermont's Motion for a Preliminary Injunction, Vermont v. Clearview AI Inc. (Vt. Super. Ct. Mar. 10, 2020).

[175] Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).

[176] Natasha Singer & Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html.

[177] Ally Marotti, *Google's Art Selfies Aren't Available in Illinois. Here's Why.*, CHI. TRIB. (Jan. 17, 2018, 7:00 AM), https://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html.

[178] *See, e.g.*, FAC, *Mutnick*, *supra* note 5, at 26.

[179] *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2008) ("Biometric identifiers do not include . . . photographs . . . . Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers."); WASH. REV. CODE ANN. § 19.375.010 (2020) ("'Biometric identifier' does not include a physical or digital photograph, video or audio recording or data generated therefrom . . . .").

[180] Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1875 (2007); Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image Over the*

upon seclusion," "public disclosure of embarrassing private facts," "publicity which places the plaintiff in a false light in the public eye," and "appropriation, for the defendant's advantage, of the plaintiff's name or likeness."[181] This Article does not aim to recapitulate others' arguments that these torts fail to address facial recognition. The next paragraph glosses, as briefly as possible, why Prosser's four torts are a poor fit for facial-recognition-related harms.

None of Prosser's torts squares very well with the harms an individual suffers when images she voluntarily published are enrolled in a facial recognition database. The tort of publicity given to private life does not apply "when the defendant merely gives further publicity to information about the plaintiff that is already public."[182] Substantially the same limitation applies to intrusion upon seclusion.[183] The false light tort makes *false* portrayals actionable, but facial recognition arguably engenders privacy harms only insofar as it uncovers *true* information that would otherwise have been obscure.[184] Finally, the most plausible claim, appropriation, is limited to uses of "the reputation, prestige, social or commercial standing" of the plaintiff's likeness.[185] A facial recognition service arguably does the opposite of appropriating a plaintiff's recognizable reputation—it instead *reveals who the plaintiff is* to customers who otherwise would have had no idea of the plaintiff's identity, reputation, or salient personal characteristics.

This Article takes it as given that most plaintiffs would have a hard time asserting any of Prosser's privacy torts against Clearview. The chief obstacle to any privacy claim is that the information Clearview enrolled in its database was, in the paradigmatic case, voluntarily published by the plaintiff. This Article's proposed tort deemphasizes the notion of a reasonable expectation of privacy, because such an expectation is probably absent in users' postings to the public Internet.[186] Instead, the

---

Internet, 49 SANTA CLARA L. REV. 313, 314 (2009); Andrew Lavoie, *The Online Zoom Lens: Why Internet Street-Level Mapping Technologies Demand Reconsideration of the Modern-Day Tort Notion of "Public Privacy,"* 43 GA. L. REV. 575, 580–81 (2009).

[181] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

[182] RESTATEMENT (SECOND) OF TORTS § 652D, cmt. b (AM. LAW INST. 1977).

[183] *Id.* at § 652B cmt. c ("The defendant is subject to liability. . . only when he has intruded into a private place . . . there is no liability for the examination of a public record concerning the plaintiff . . . [n]or is there liability for observing him or even taking his photograph while he is walking on the public highway . . . .").

[184] *See id.* at § 652E Perhaps a plaintiff could assert a false light claim arising out of a *mis*identification by a facial recognition algorithm, but such a possibility is beyond this Article's scope.

[185] *Id.* at § 652C cmt. c.

[186] *See, e.g.*, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 994 (9th Cir. 2019) ("[T]here is little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly, and it is doubtful that they do.").

proposed tort emphasizes justifiable expectations about control over that information—specifically, the expectation that third parties will not collect published information in a manner and/or for a purpose that violates terms of service that bind both the users and the third party. By recharacterizing the harm users suffer in Clearview-like scenarios, this Article's proposed tort sidesteps the "expectation of privacy" formulations that may disqualify established privacy torts. Instead, it emphasizes expectations predicated on contractual terms.

3. Unjust Enrichment

Some of the lawsuits filed against Clearview by platform users allege unjust enrichment.[187] This cause of action avoids many of the conceptual disadvantages of the property, intellectual property, or established tort claims that this Article describes. Unlike intellectual property theories of recovery, which previous sub-Sections suggest are misguided, unjust enrichment theories better recognize that the information Clearview allegedly scraped is nonproprietary. Accordingly, and advantageously, its theory of recovery is *relational*: like this Article's proposed tort of bad faith breach, it attaches to Clearview in particular because the company behaved in a wrongful manner. The crucial difference between unjust enrichment and this Article's proposed tort is that the former focuses on the defendant's enrichment *at a plaintiff's expense*, while the latter focuses on the wrongness of the defendant's conduct. This theoretical difference deserves emphasis, even if its practical significance is comparatively small: subsequent Sections will argue that restitution—quintessentially the remedy for unjust enrichment[188]—may also be an appropriate remedy for the wrong this Article describes.

The normative tenets of unjust enrichment are elementary: for example, "a person is not permitted to profit by his own wrong."[189] But the doctrine and nomenclature of unjust enrichment are contested, and they reflect convoluted legal conventions that evolved from arcane procedural rules.[190] Some scholars argue that unjust enrichment and restitution "quadrate:" that is, restitution is a remedy available only in cases of unjust enrichment, and unjust enrichment gives rise only to restitutionary remedies.[191] Others disaggregate unjust enrichment from restitution:

---

[187] Complaint at 26, Burke v. Clearview AI, Inc., No. 20-cv-00370-BAS-MSB (S.D. Cal. Feb. 27, 2020); FAC, *Mutnick*, *supra note* 5, at 29.

[188] *See* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 (AM. LAW INST. 2011) ("A person who is unjustly enriched at the expense of another is subject to liability in restitution.").

[189] *See id.* at § 3.

[190] *See, e.g.*, Arthur Corbin, *Waiver of Tort and Suit in Assumpsit*, 19 YALE L.J. 221, 221 (1910) ("[I]t is a subject in which there has always been great confusion of thought, and the decisions are in hopeless conflict. This is due to the fact that the substantive principles of the common law were developed as mere incidents to forms of action and procedure.").

[191] *See, e.g.*, Andrew Burrows, *Quadrating Restitution and Unjust Enrichment: A Matter of*

the former is a *cause*, the latter is a *remedy* that may arise from causes other than unjust enrichment.[192]

To the extent this Article has a dog in the fight, it follows the latter, multi-causal account of restitution, propounded most famously by Peter Birks. On Birks's framing, restitution is a remedy that may be caused by a defendant's unjust enrichment, but may also arise from a wrong a defendant commits against a plaintiff.[193] Treating restitution as a possible remedy for a wrong—rather than just the flipside of unjust enrichment—allows this Article to focus on explaining why Clearview's alleged conduct was wrong, and then using that wrong as the basis for a remedy in restitution.

Identifying a wrong is easier than pinpointing precisely why Clearview was enriched *at individuals' expense*, which is what an unjust enrichment theory would typically require.[194] Because facial recognition information is non-rivalrous and non-proprietary, it may be difficult to argue how its usage in facial recognition software occurs at the expense of its subjects, independent of a privacy wrong. Thus, while it avoids some difficulties of an unjust enrichment theory, this Article's proposed wrong does not necessarily foreclose restitutionary remedies that plaintiffs might pursue.[195]

Unjust enrichment allows courts to provide a remedy when one individual "is unjustly enriched at the expense of another."[196] Unjust enrichment may result from two parties behaving non-culpably—for example, a plaintiff mistakenly remitting a debt to the wrong person. Recovery for unjust enrichment might typically amount

---

Principle?, 8 RESTITUTION L. REV. 257, 258 (2000).

[192] *See* Peter Birks, *Unjust Enrichment and Wrongful Enrichment*, 79 TEX. L. REV. 1767, 1770 (2000).

[193] *Id.*

[194] *Cf. id.* at 1783–84. Instructively, Birks cites Hart v. E.P. Dutton & Co., 93 N.Y.S.2d 871, 873–74, 880 (N.Y. Sup. Ct. 1949), to illustrate a potential difficulty of deriving enrichment "at the expense of" a plaintiff independent from a wrong the defendant has committed. In *Hart*, the plaintiff Hart sued the publisher of a book that, he claimed, libeled him. Hart sought a restitutionary award of the publisher's profits, but the court held that his claim was barred by the one-year statute of limitations on libel, which had expired, and not by a six-year limitation on implied contract claims. Birks writes of *Hart*,

> This must be right. He was claiming a restitutionary award, but the ground of his claim was still the tort of libel . . . . Alternative analysis in unjust enrichment would have required, *inter alia*, that Hart satisfy the phrase "at the expense of" without relying on any wrong. He would then have had to find an unjust factor which was also distinct from the wrong. There is no evidence that he attempted to do that, and it probably could not have been done.

Id.

[195] *Cf.* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 44 cmt. b ("Profitable interference with other protected interests, such as the claimant's right of privacy, gives rise to a claim under § 44 if the benefit to the defendant is susceptible of measurement.").

[196] *Id.* at § 1; *see also, e.g.*, Ghirardo v. Antonioli, 924 P.2d 996, 1003 (Cal. 1996).

to the value of the services rendered (*quantum meruit*), or the return of a particular piece of property.[197] When a defendant has behaved culpably, he may be required to disgorge his profits to the plaintiff.[198]

As applied to the Clearview situation, then, unjust enrichment is an imperfect fit. What makes Clearview's alleged conduct categorically different from, say, hiQ's, is that Clearview allegedly scraped information to use it for a purpose Facebook *expressly represented it would not do*.[199] While LinkedIn and hiQ sought to provide competing employee analytics services using the same data, Clearview transgressed *vis-à-vis* Facebook and its users by undertaking to do something the other parties had agreed *not* to do.[200] If we assume that the aggrieved users would not have licensed their images for enrollment in a facial recognition database for law enforcement and industry, then Clearview did not simply enrich itself by scraping information that it could have obtained transactionally. Put another way, Clearview did not obtain the sort of unjust enrichment that the Supreme Court cited as the basis for the right of publicity: "unjust enrichment by the theft of good will . . . get[ting] free some aspect of the plaintiff that would have market value and for which [defendant] would normally pay."[201] Rather, Clearview allegedly scraped data for a purpose explicitly rejected by Facebook's compact with its users.[202]

On this framing, Clearview cannot just pay the market value of data that plaintiffs would have been entitled to receive, or restore the devaluation of that data attributable to Clearview's use.[203] Internalizing value that individual Internet users could have collected through a consensual license may be unjust. But internalizing

---

[197] *See* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT §§ 49, 54–55; Meister v. Mensinger, 178 Cal. Rptr. 3d 604, 618 (Cal. Ct. App. 2014); Maglica v. Maglica, 78 Cal. Rptr. 2d 101, 104 (Cal. Ct. App. 1998).

[198] *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 51; *cf.* WARD FARNSWORTH, RESTITUTION: CIVIL LIABILITY FOR UNJUST ENRICHMENT 112 (2014) (discussing "blameworthy defendants").

[199] *How Do I Turn the Face Recognition Setting On or Off for My Facebook Account?*, FACEBOOK HELP CTR., https://www.facebook.com/help/187272841323203?helpref=faq_content (last visited Feb. 27, 2021).

[200] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 998 (9th Cir. 2019) ("[LinkedIn's] decision to send a cease-and-desist letter occurred within a month of the announcement by LinkedIn's CEO that LinkedIn planned to leverage the data on its platform to create a new product for employers with some similarities to hiQ's Skill Mapper product.").

[201] Harry Kalven, Jr., *Privacy in Tort Law: Were Warren and Brandeis Wrong?*, 31 L. & CONTEMP. PROBS. 326, 331 (1966), *cited in* Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 576 (1977).

[202] *How Do I Turn the Face Recognition Setting On or Off for My Facebook Account?*, *supra* note 199.

[203] *See* Balganesh, *supra* note 169, at 467 (discussing "correspondence approach" to determining when a plaintiff has conferred a benefit on a defendant in an unjust enrichment action).

value with the knowledge that Internet users would have refused to surrender it in the marketplace is *wrongful*.[204] Indeed, the logic of an unjust enrichment claim suggests a baseline propriety to market transactions in facial recognition data for law enforcement use—but the outrage the Clearview episode has provoked, and major platforms' prolonged forbearance from creating such technologies, is premised on the present-day *im*propriety of such transactions.

An unjust enrichment theory is a near match for the Clearview scenario, but it risks imposing rationales of property and markets onto non-proprietary information that had been explicitly withheld from the facial-recognition-as-a-service market. Because unjust enrichment doctrine is so contested and confused, it may offer a route to substantially the same results as this Article's proposed tort. The point of the past ten paragraphs or so of semantic wrangling, then, has been to avoid characterizing biometric information as just another alienable asset and to set up a serious analysis of why Clearview's alleged behavior was *wrong*. Concluding that Clearview's enrichment was unjust begs the question of wrongfulness. Instead of trying to describe how Clearview's gains accrued at users' expense, subsequent Sections of this Article describe why Clearview's alleged conduct can be described as wrongful. That wrong, in turn, could provide a route to the restitution remedy that an unjust enrichment claim might have yielded.[205]

D. Platforms' Relational Interests

Platforms are not out of luck if neither the CFAA nor the common law of trespass covers scraping of the public web. Instead, as both the Ninth Circuit and Kerr observe, companies may invoke contract law against entities that breach their terms of service.[206] Moreover, the market-orientated rationales of misappropriation and unjust enrichment that make those doctrines inapt for addressing users' privacy grievances may actually make them apt for redressing companies' losses.

An appropriate theory of recovery for companies will emphasize the relational nature of companies' rights against scrapers. This Section's sub-Section on property emphasized that an *in rem*, nonrelational right is an inappropriate mechanism for policing non-interfering access to public servers and the reproduction of publicly-available facts. A relational remedy—whether flowing from the defendant's actions as a party to a contract with a plaintiff platform, or more generally as a competitor to that platform—properly focuses on the impropriety of *a particular defendant* accessing information *by particular means*.

---

[204] *See* Birks, *supra* note 192, at 1783.

[205] *See also* FARNSWORTH, *supra* note 198, at 61–62 (discussing the relationship between restitution and tort); *see infra* Section V.

[206] Kerr, *supra* note 151, at 1170 ("Companies can already use civil contract law, based on terms of use, to set legal limits on how visitors use their websites.").

Such a relational approach has numerous virtues. It avoids "propertizing" nonproprietary information, and it rightly avoids remedying non-trespassory interactions with servers as if they were trespasses to tangible property. Instead, causes of action that focus on a relationship between particular parties and the actions of those particular parties can, as Shyamkrishna Balganesh suggests of misappropriation doctrine, "allow courts to modulate and balance the entitlement against free speech and other concerns."[207]

V. THE TORT OF BAD FAITH BREACH OF TERMS OF SERVICE

The common law of California can support a narrow, relational claim against entities that willfully violate a platform's terms of service, to the detriment of claimants who rely on those same terms in separate agreements with the platform. In other words, in spite of the inadequacy of the claims the previous Section surveyed, individual plaintiffs should be able to state a tort claim against Clearview. This Section elaborates that cause of action in four stages.

First, it outlines the problem that the tort addresses: users of Internet platforms lack the rights to enforce covenants in the terms of service that protect the users' own interests. Instead, those users must trust the platforms to enforce those covenants against third parties that breach them, even when platforms' incentives to do so diverge from users'. Second, it argues that relevant California precedent supports reading bilateral terms of service contracts to create a narrow duty to third parties not to breach certain covenants. Third, it explains that the willful breach of such a duty can be grounds for awarding tortious damages. Fourth, and finally, it describes the elements of the proposed tort and responds to threshold objections.

A. The Trust-Your-Overlords Problem

The relationship between a major Internet platform and its users looks a little bit like feudalism.[208] It is difficult, if not impossible, for an ordinary person to maintain a social and professional presence online without delegating its technological administration to third parties. This delegation brings immense benefits: for instance, Gmail relieves end users of the part-time job of administering one's own email server.[209] And someone committed to rolling-one's-own services would be

---

[207] Balganesh, *supra* note 169, at 495.

[208] *See generally* Katrina Geddes, *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, 43 COLUM. J.L. & ARTS 455, 455–56 (2020); Bruce Schneier, *When It Comes to Security, We're Back to Feudalism*, WIRED (Nov. 26, 2012, 06:30 AM), https://www.wired.com/2012/11/feudal-security/.

[209] *See* Lee Hutchinson, *How to Run Your Own E-mail Server with Your Own Domain, Part 1*, ARS TECHNICA (Feb. 16, 2014, 6:00 PM), https://arstechnica.com/information-technology/2014/02/how-to-run-your-own-e-mail-server-with-your-own-domain-part-1/.

unable to participate at all on a closed social network like Facebook.

But the delegation to companies also has downsides. The first is difficulty of preference-satisfaction: users may find it difficult to find a package of services that suits their precise preferences for functionality, privacy, and security. Another is lack of control over the bargain: the biggest platforms offer end-users *gratis* services in exchange for essentially unfettered access to user data.[210] A third downside is inflexibility: once a user adopts a platform, a lack of data portability may make it onerous to switch providers.[211]

Combining platforms' advantages (irrefutable economies of scale and social indispensability) with their disadvantages (difficulties in preference-satisfaction, lack of control, and lock-in effects) reveals the feudal aspects of the status quo. Most Internet users have no practical option other than to use at least one major platform. And once users rely on one platform, they must rely on the proprietors of that platform to protect their interests. Some of that protection may come from promises the platforms make to users about how users will be treated. Those promises appear in platforms' Terms of Service, and users do retain some ability to enforce them against platforms.[212]

Some of what users delegate to platforms is their ability to protect themselves against third parties' malfeasance. Imagine that instead of a centralized service, LinkedIn offered a federated protocol that allowed individual users to create profiles on servers that the users themselves owned and operated personally, and then to identify and connect with other similarly-situated users.[213] Such a service—call it LinkedOut—could allow each user to set the terms on which third parties may interact with her profile and her server. If a third party—say, a data scraper—accepted a LinkedOut user's personal terms, and then violated those terms, the LinkedOut user might have contractual or statutory recourse against that third party. In contrast, LinkedIn users must rely on LinkedIn itself to enforce *its* terms against a third party that violates those terms. This hub-and-spoke structure of contracts puts a platform at the center of a network of users who are in privity with the platform but not with one another. It engenders what might be called the "trust-your-overlords" problem.

---

[210] Zeynep Tufekci, *Mark Zuckerberg, Let Me Pay for Facebook*, N.Y. TIMES (June 4, 2015), https://www.nytimes.com/2015/06/04/opinion/zeynep-tufekci-mark-zuckerberg-let-me-pay-for-facebook.html.

[211] Schneier, *supra* note 208.

[212] *See, e.g.*, *In re* Facebook, Inc., Consumer Privacy User Profile Litig., 402 F. Supp. 3d 767, 801 (N.D. Cal. 2019) (holding that Facebook users stated claim for breach of contract arising out of Facebook's alleged noncompliance with its Data Use Policy).

[213] *See generally* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, KNIGHT FIRST AMEND. INST. (Aug. 21, 2019), https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech.

The trust-your-overlords problem is that users may rely on centralized platforms' terms when entering into relationships with that platform, and those terms may reasonably influence the users' expectations of how others bound by the terms will interact with the platform. But if a second user interacts with the platform in a way that violates the platform's terms—short of committing an established tort against the first user—the user must depend on the platform itself to enforce its terms against the breaching user. These issues are particularly salient in the field of content moderation. Some Twitter users, for example, are outraged that flagrant violations of Twitter's rules against hate speech go undisciplined by Twitter.[214] However, they must rely on their overlords to enforce those rules.

The same would appear to be true of users who are aggrieved by Clearview's face-scraping operations. Clearview has received cease-and-desist notices for violating Facebook's and Twitter's terms of service. But ultimately, only the platforms, not their users, would ordinarily have the ability to enforce their terms against a willfully breaching party.

Feudalism may not be so bad if one can actually rely on one's overlords for protection in a perilous world. Indeed, that pledge of protection is more or less the *point* of feudalism, at least as far as vassals are concerned.[215] But the facts of the Clearview situation suggest that trust in one's overlords might be misplaced: Clearview reportedly received funding from Peter Thiel, who is also on Facebook's board of directors.[216] Facebook users may have relied on Facebook's pledges to limit its use of facial recognition technology in choosing whether to join the network.[217] Now that a third party—one that may have been bound by Facebook's terms, including Facebook's prohibition on automated data collection—has undermined those expectations willfully, must users depend only on not-so-disinterested Facebook to redress the problem by enforcing its terms against Clearview?

1. The Information Fiduciary Response

Jack Balkin and Jonathan Zittrain have identified the shortcomings of the

---

[214] Kara Swisher, *Rules Won't Save Twitter. Values Will.*, N.Y. TIMES (Aug. 8, 2018), https://www.nytimes.com/2018/08/08/opinion/twitter-alex-jones-jack-dorsey.html.

[215] Elizabeth A.R. Brown, *Feudalism*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/feudalism (last visited Jan. 27, 2021).

[216] Hill, *supra* note 1; *see also* Jonathan Zittrain (@zittrain), TWITTER (Jan. 18, 2020, 6:44 AM), https://twitter.com/zittrain/status/1218544819615780864 ("If the article is right that a Facebook board member has invested in the company that's gathering these photos as its core business, against Facebook's own terms of service, I'd want to think more about whether that's a violation of that board member's fiduciary duty to Facebook.").

[217] *See What Is the Face Recognition Setting on Facebook and How Does It Work?*, FACEBOOK, https://www.facebook.com/help/122175507864081?helpref=faq_content (last visited Jan. 27, 2021).

trust-your-overlords paradigm and have proposed addressing it by imposing a fiduciary duty on Internet platforms that handle the sensitive personal information of end users.[218] In fact, in an amicus brief to the Ninth Circuit in *hiQ*, the Electronic Privacy Information Center (EPIC) argued that "LinkedIn's user agreement and privacy policy establish a fiduciary relationship with users" under which "LinkedIn bears the burden of protecting a user's personal information and ensuring data is only collected, used, and disclosed consistent with the company's terms, settings, and LinkedIn's representations."[219] In reply to information fiduciary proposals, others have observed that fiduciary duties do not transpose neatly onto the more nuanced obligations that platforms may assume towards users, such as content-moderation.[220] Critics of the proposed fiduciary model note that it does little to address the circumstances that engendered the trust-your-overlords problem in the first place: instead of working to counter major platforms' market power and their economic incentives to disregard users' privacy interests, it "conceives of systemic problems in relational terms."[221]

This Article's proposal is far more modest than an information fiduciary obligation. First, it applies only in narrow circumstances. Second, it modifies not the ubiquitous contractual relations between platforms and their users, but rather the relations between users and peripheral actors that willfully undermine the protections that platforms represented to their users. That means that, on its own, the proposal comes nowhere close to redressing the interconnected harms that extractive Internet platforms may wreak on users, the broader commercial ecosystem, or democratic society at large. But these limitations are also advantages. This proposal's modesty helps it avoid some of the internal incoherence that critics identify in proposals for information fiduciaries. And its limited scope makes it far easier to implement: Instead of a sweeping reform that might preempt existing privacy regulations and demand novel enforcement techniques, this cause of action would require nothing more than a common law judge's imprimatur.[222]

---

[218] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1221–24 (2015); *see also* Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/.

[219] Brief of Amicus Curiae Electronic Privacy Info. Ctr. (EPIC) in Support of Neither Party Urging Reversal at 13, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019) (No. 17-16783).

[220] James Grimmelmann, *When All You Have Is a Fiduciary*, L. & POL. ECON. (May 30, 2019), https://lpeblog.org/2019/05/30/when-all-you-have-is-a-fiduciary/.

[221] Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 535 (2019).

[222] *See id.* at 509; *see also* Balkin, *supra* note 218.

B. Bilateral Terms of Service Can Create Duties to Third Parties

To make actors like Clearview liable to aggrieved plaintiffs, it is helpful to have a precise account of what Clearview allegedly did that was "wrong," and why a particular plaintiff ought to be entitled to redress for that wrong.[223] The following two Sections argue that platforms' terms of service can structure users' expectations, interests, and behaviors such that intentionally violating those terms may wrong users who are parties to parallel instantiations of the same terms. In other words, people participate in commercial social networks because they understand that other users are bound by the same terms they accept. Therefore, in some cases, one user's violations of an obligation under the terms can amount to a wrong against another user.[224]

This Section explains that California caselaw offers a doctrinal basis for recognizing that bilateral terms of service can give rise to a legal duty to avoid such wrongs to users. As deployed to establish duties in negligence suits, this line of cases has been criticized as analyzing "open-ended *policy* questions about appropriate levels of *liability*" rather than determining appropriate *legal* questions of *responsibility*.[225] But the same legal analysis helps explain, both theoretically and doctrinally, why *intentionally* violating a covenant in a platform's terms of service can be understood as a legal wrong to a user of that platform.

As a "matter of policy," California courts sometimes grant nonparties to a contract the right to sue for a contracting party's inadequate performance.[226] The California Supreme Court introduced this analysis in *Biakanja v. Irving*, which held that the beneficiary of a will could recover damages against a notary whose negligence rendered the will invalid, despite the plaintiff not being in privity with the

---

[223] *See* John C.P. Goldberg & Benjamin C. Zipursky, *Torts as Wrongs*, 88 TEX. L. REV. 917, 937–39 (2009).

[224] This is not to say that violating a provision of a terms of service agreement is the only possible basis on which an actor like Clearview could be said to have committed a legal wrong against an individual user of a social network. There are many plausible ways to state why enrolling someone in a commercial facial recognition database without that person's consent is wrongful. This particular explanation tries to give the account legal and substantive force by anchoring it in familiar legal forms. Deriving a duty to users from a covenant in a platform's terms of service is just one explanation for why conduct that happens to violate that covenant may be wrongful. This explanation is analytically disciplined and tailored to this Article's purposes, but it should not be understood to exclude or conflict with other, broader explanations of why Clearview's alleged conduct has wronged Internet users. For further discussion of this proposal's self-consciously limited scope, *see infra* Section V.E.2.

[225] John C.P. Goldberg & Benjamin C. Zipursky, *Shielding Duty: How Attending to Assumption of Risk, Attractive Nuisance, and Other "Quaint" Doctrines Can Improve Decisionmaking in Negligence Cases*, 79 S. CAL. L. REV. 329, 330 (2005).

[226] Biakanja v. Irving, 320 P.2d 16, 19 (Cal. 1958).

notary.[227] *Biakanja* set forth the following factors for determining whether to impose a duty on a noncontracting party:

> [1] the extent to which the transaction was intended to affect the plaintiff, [2] the foreseeability of harm to him, [3] the degree of certainty that the plaintiff suffered injury, [4] the closeness of the connection between the defendant's conduct and the injury suffered, [5] the moral blame attached to the defendant's conduct, and [6] the policy of preventing future harm.[228]

Citations to *Biakanja* often occur in the context of recovery for purely economic losses.[229] Notably, however, at least one court has invoked *Biakanja*'s duty analysis in the context of emotional harm, as well.[230] The following sub-Sections analyze each factor to argue that certain covenants in a platform's bilateral terms of service should create duties to third parties that are also in privity with a platform. While the analysis below tracks California's test, numerous other jurisdictions have cited *Biakanja* favorably and applied similar balancing tests to derive duties—albeit often extremely limited ones—to nonparties arising from contractual relationships.[231]

---

[227] *Id.* at 17.

[228] *Id.* at 19, *cited with approval in* Centinela Freeman Emergency Med. Assocs. v. Health Net of Cal., Inc., 382 P.3d 1116, 1128 (Cal. 2016).

[229] *See, e.g.*, J'Aire Corp. v. Gregory, 598 P.2d 60, 63 (Cal. 1979).

[230] *See* Andalon v. Superior Court, 162 Cal. App. 3d 600, 610–11 (1984) (analyzing "along *Biakanja* lines" a nonpatient's claim against a doctor for negligent infliction of emotional distress: "The tort duty arising from the contract [between defendant doctor and plaintiff's spouse] runs to [plaintiff], not merely because of the forseeability of emotional harm to [plaintiff], but because of the nexus between his significant interests and the 'end and aim' of the contractual relationship.").

[231] *Cf., e.g.*, Harrigfeld v. Hancock, 90 P.3d 884, 889 (Idaho 2004) (articulating "very narrow" duty of lawyers to certain testamentary beneficiaries); Leyba v. Whitley, 907 P.2d 172, 177 (N.M. 1995) ("[W]e join those jurisdictions that have rejected any stringent privity test as the touchstone of an attorney's duty to a nonclient."); Sentry Select Ins. v. Maybank Law Firm, LLC, 826 S.E.2d 270, 274 (S.C. 2019) (recognizing a legal malpractice claim outside strict privity as "a matter of policy . . . involv[ing] the balancing of various factors") (internal citations omitted); Erpelding v. Lisek, 71 P.3d 754, 758 (Wyo. 2003). *But cf.* Annett Holdings, Inc. v. Kum & Go, L.C., 801 N.W.2d 499, 504 (Iowa 2011) ("When parties enter into a chain of contracts, even if the two parties at issue have not actually entered into an agreement with each other . . . tort law should not supplant a consensual network of contracts."); Noble v. Bruce, 709 A.2d 1264, 1271 (Md. 1998) (criticizing *Biakanja*'s "balancing of factors approach" as "broad" and "unworkable").

1. Anti-Scraping Covenants Arguably Exist for Users' Benefit

Major platforms' terms of service almost always disclaim any third-party beneficiary rights.[232] Facebook's and Google's do so as explicitly as possible.[233] Twitter's terms imply that they do not create third-party beneficiary rights.[234] An explicit disclaimer of third-party benefit is about the strongest possible indication that these platforms' terms of service are not intended to benefit individual users suing Clearview. This Article does not want to overstate its case: these disclaimers would be difficult to surmount. A court might well find them fatal to this author's proposal. But there are good arguments that the four corners of these terms do not reflect the parties' complete intentions.

It makes intuitive sense that some provisions of platforms' terms of service exist for the benefit of other users. Michael Risch has argued for a "broad reading of intended beneficiary status" in platforms' terms of service on this basis.[235] Risch proffers several common provisions that seem obviously intended to benefit third-party users. For example, third-party users "objectively benefit" from anti-cheating clauses in multiplayer games, anti-spam or anti-harassment clauses, and clauses in which service providers promise not to regulate users' interactions beyond the interventions the terms enumerate.[236] Thus, the substance of terms of service would seem to belie platforms' claims that the contracts are not intended to benefit third-party users.

Moreover, the representations about beneficiaries that platforms make to courts sometimes diverge from the letter of their terms. LinkedIn's own briefing describes how the configuration of its robots.txt file "benefits members"[237] and asserts that "LinkedIn restricts automated bots from making tens of millions of calls to its servers to extract data. This both protects members' privacy interests, and the

---

[232] James Grimmelmann, *Third Parties to the Rescue*, JOTWELL (Nov. 9, 2009), https://cyber.jotwell.com/17/ ("I suspect that the moment courts start to recognize users' rights to enforce user agreements against each other, companies will immediately rewrite their terms of service to expressly disclaim any possible third-party benefits.").

[233] *Terms of Service*, FACEBOOK, https://www.facebook.com/legal/terms/plain_text_terms (last visited Feb. 27, 2021) ("These Terms do not confer any third-party beneficiary rights."); *Google Terms of Service*, GOOGLE, https://policies.google.com/terms?hl=en-US (last visited Feb. 27, 2021) ("These terms describe the relationship between you and Google. They don't create any legal rights for other people or organizations . . . .").

[234] *Twitter Terms of Service*, TWITTER, https://twitter.com/en/tos (last visited Jan. 27, 2021) ("This license has the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Twitter, in the manner permitted by these Terms.").

[235] Michael Risch, *Virtual Third Parties*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 416, 425 (2009).

[236] *See id.* at 422–25.

[237] Appellant's Opening Brief at 7 n.1, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019) (No. 17-16783).

LinkedIn website itself from technical overload and other problems."[238] And in CFAA litigation against a company that accessed its network without authorization, Facebook described the terms of the "Facebook Connect" developer platform as "designed to safeguard users' privacy and data."[239]

Of course, positions taken in litigation regarding a contract do not nullify that contract's explicit language. But those positions are not meaningless ephemera, either. Courts have equitable discretion to hold parties estopped from "playing fast and loose with the courts" by asserting incompatible claims.[240] The district court in *hiQ* explicitly noted inconsistencies between LinkedIn's position in that case and the positions LinkedIn had taken in prior litigation.[241] Because LinkedIn had argued in other litigation that its users cannot claim a privacy interest in information that they post publicly to LinkedIn, the district court looked skeptically upon LinkedIn's argument that it sought to curtail hiQ's scraping "solely out of concern for member privacy[,]" rather than for anticompetitive purposes.[242] Thus, disclaimers notwithstanding, there are practical reasons and doctrinal mechanisms for recognizing that platforms' scraping prohibitions exist at least partially for users' benefit.

2. Privacy Harm Is a Foreseeable, Certain, and Proximate Consequence of Nonconsensual, Commercial Facial Recognition

It is easily foreseeable that Clearview's willful breach of a platform's anti-scraping terms, for the purposes of creating a facial recognition service for law enforcement, could harm the affected users. For one, precedent acknowledging a similar harm is readily available. In *Patel v. Facebook*, Facebook users mounted a class action against Facebook for storing their facial-recognition data for use as photo-tagging suggestions, which settled in January 2020 for $550 million.[243] Although that liti-

---

[238] LinkedIn Corp.'s Supplemental Brief in Opposition to Plaintiff's Motion for a Preliminary Injunction at 16, hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099 (N.D. Cal. 2017) (No. 17-CV-03301-EMC).

[239] Facebook, Inc.'s Reply to Amicus Curiae Electronic Frontier Foundation's Brief in Support of Defendant Power Ventures' Motion for Summary Judgment at 1, Facebook, Inc. v. Power Ventures, Inc., 252 F. Supp. 3d 765 (N.D. Cal. 2017) (No. 08-CV-05780-LHK).

[240] *See* New Hampshire v. Maine, 532 U.S. 742, 750 (2001) (quoting Scarano v. Central R.R. Co., 203 F.2d 510, 513 (3d Cir. 1953)) (internal quotations omitted); *see also, e.g.*, Williamson v. Williamson, 657 N.E.2d 651, 657 (Ill. App. Ct. 1995) (surveying equitable doctrine against approbation and reprobation).

[241] hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1118 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019).

[242] *Id.*

[243] *See* Singer & Isaac, *supra* note 176; Rachel Pester, *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit*, JOLT DIGEST (Feb. 14, 2020), https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-

gation proceeded under the Illinois Biometric Information Privacy Act (BIPA), rather than a common law privacy tort, the Ninth Circuit concluded for the purposes of Article III standing "that an invasion of an individual's biometric privacy rights has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[244]

Importantly, *Patel* characterized "the development of a face template using facial-recognition technology without consent" as an invasion of a *privacy* interest.[245] "[B]oth the common law and the literal understandings of privacy," the Ninth Circuit observed, "encompass the individual's control of information concerning his or her person."[246] The court contemplated that "the facial-recognition technology at issue here can obtain information that is 'detailed, encyclopedic, and effortlessly compiled,'" and which could serve to track someone's individual movements, identify her associates, or potentially even bypass the biometric authentication measures that secure her cell phone.[247]

Patel's conception of privacy, then, suggests that the interest Clearview allegedly invaded may properly be called a privacy interest. The public availability of photos posted to social media websites does not necessarily vitiate any privacy interests the users might retain in how those photos are collected and processed. Rather, collection and processing of those photographs in a manner and for a purpose rejected by a platform's terms of service encroaches on those individuals' "*control of information concerning [their] person.*"[248] Such scraping disregards the informational controls—the prohibitions of scraping and of most facial recognition usage—memorialized in platforms' agreements with their users.

Moreover, Clearview's alleged conduct is far more harmful than Facebook's allegedly injurious uses of facial recognition. Facebook users were found to be injured merely because Facebook used facial recognition to suggest an individual to be tagged in an uploaded photograph. In contrast, Clearview reportedly provides its products to law enforcement and private industry, and operates without the consent of effectively every person in its database.

Interpretations of *Biakanja*'s "certainty" prong tend to operate to limit the sphere of eligible plaintiffs rather than to determine whether or not to recognize a cause of action at all. In a case involving widespread mishandling of corpses in the funeral business, the California Supreme Court subsumed certainty into its foreseeability analysis and limited a plaintiff class to those who were aware of their relatives'

---

information-privacy-act-bipa-violation-suit.

244 Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019) (internal citations omitted).

245 *Id.*

246 *Id.* (quotation marks omitted).

247 *See id.*

248 *Cf. id.* (emphasis added).

burial, even if they did not personally witness the misconduct firsthand.[249] This factor may therefore limit potential plaintiffs to those who can adequately plead a privacy harm caused by Clearview's willful breach of platforms' terms. It is likely that at least some suitable plaintiffs can plead such damages, given the general moral opprobrium that surrounds Clearview's practices.[250]

Biakanja's close connection requirement acts as a screen for remote consequences of negligence, rather than a restriction on liability for intentional conduct. Although Clearview may have been merely reckless, rather than intentional, concerning the privacy harms that its activities caused to users, Clearview's actions alone are the direct and proximate cause of the scenario plaintiffs might plausibly find injurious. The California Supreme Court has found a sufficiently close connection to impose a duty even when a party other than the defendant was "the immediate and direct cause of plaintiff's economic injury."[251] The California Supreme Court neglected to find a connection between an escrow agent's alleged negligence and a financial loss it caused to a nonparty to the escrow, on the grounds that the nonparty's injury was attributable at least in part to its own noncompliance with a statutory obligation.[252] In this case, Clearview's purpose in breaching the terms of Internet platforms was to construct a facial recognition database, and it was the creation and commercial use of that database that caused Internet users' grievances.

3. Clearview's Alleged Conduct Is Morally Blameworthy

Clearview's alleged conduct is blameworthy in a variety of relevant senses of the word. First, networking experts frequently describe as unethical behavior that violates the preferences that server owners express in the robots.txt exclusion standard. As far back as 25 years ago, computer scientists proposed that an "ethical" interaction with a server should "respect the constraints placed upon it by server operators."[253] Adherence to, or violation of, the robots.txt exclusion protocol remains a criterion for the "ethicality" of web crawlers.[254] It is not clear whether Clearview

---

[249] Christensen v. Superior Court, 820 P.2d 181, 196–97 (Cal. 1991).

[250] *See infra* Section V.B.3.

[251] *See* Centinela Freeman Emergency Med. Assocs. v. Health Net of Cal., Inc., 382 P.3d 1116, 1129 (Cal. 2016).

[252] Summit Fin. Holdings, Ltd. v. Cont'l Lawyers Title Co., 41 P.3d 548, 554–55 (Cal. 2002).

[253] David Eichmann, *Ethical Web Agents*, 28 COMPUTER NETWORKS & ISDN SYS. 127, 133–34 (1995).

[254] Yang Sun et al., *The Ethicality of Web Crawlers*, 2010 IEEE/WIC/ACM INT'L CONF. ON WEB INTELLIGENCE & INTELLIGENT AGENT TECH. 668, 668 (IEEE Toronto, AB, Canada Aug. 2010).

complied with the robots.txt instructions of servers it visited.[255] hiQ's activities apparently did not comply with the instructions in LinkedIn's robots.txt file.[256]

Second, Clearview's business practices suggest an awareness that its conduct violated prevailing norms. It listed a fake address as its place of business, and its CEO used a pseudonym.[257] Clearview also instructed police departments that used its services not to discuss them with the media, and appeared to modify its results to hinder a reporter's efforts to identify herself.[258] While clandestine operations may also be consistent with prudent business sense, they reinforce the view that Clearview understood that its conduct would attract disapproval if it were more widely known.

Third, popular reactions to the Clearview revelations suggest that its conduct is blameworthy. The Vermont Attorney General asserted in a recent court filing that Clearview's alleged conduct is "highly offensive and a 'breach of social norms.'"[259] In a letter to Clearview, Senator Ed Markey wrote, "Clearview's product appears to pose particularly chilling privacy risks, and I am deeply concerned that it is capable of fundamentally dismantling Americans' expectation that they can move, assemble, or simply appear in public without being identified."[260] A CBS News feature on Clearview that aired shortly after Hill's *exposé* described the technology as "rais[ing] sobering moral and ethical questions."[261]

Fourth, and perhaps most crucially, the relationship between the scraper's conduct and the platform's own practices can illuminate the appropriate degree of blame. It can also distinguish the facts of *hiQ* from those of Clearview in a potentially dispositive way. In *hiQ*, the parties were disputing the *price* of the data at issue,[262] not whether anyone could perform the analytics service that hiQ performed. The Ninth Circuit noted in *hiQ* that "there is evidence that LinkedIn has itself developed a data analytics tool similar to hiQ's products, undermining LinkedIn's

---

[255] Tim Cushing, *Google Says Clearview's Site Scraping Is Wrong; Clearview Reminds Google It Scrapes Sites All the Time*, TECHDIRT (Feb. 6, 2020), https://www.techdirt.com/articles/20200205/14263943864/google-says-clearviews-site-scraping-is-wrong-clearview-reminds-google-it-scrapes-sites-all-time.shtml.

[256] Appellant's Opening Brief at 7, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019) (No. 17-16783).

[257] Hill, *supra* note 1.

[258] Kashmir Hill, *Unmasking a Company that Wants to Unmask Us All*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/reader-center/insider-clearview-ai.html.

[259] State of Vermont's Motion for a Preliminary Injunction at 32, Vermont v. Clearview AI Inc. (Vt. Super. Ct. Mar. 10, 2020) (quoting *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 129 (3d Cir. 2015)).

[260] Markey to Ton-That, *supra* note 7.

[261] CBS News, *CEO Speaks Out About Clearview AI's Controversial Facial Recognition Technology* at 2:12, YOUTUBE (Feb. 5, 2020), https://www.youtube.com/watch?v=-JkBM8n8ixI.

[262] I am grateful to Rebecca Tushnet for framing the issue in these terms.

claim that it has its members' privacy interests in mind."[263] In other words, hiQ's conduct did not pose a harm to LinkedIn users that differed in kind from an activity that LinkedIn itself would have undertaken. hiQ's analytics service may not have given LinkedIn users exactly the degree of control over their information that LinkedIn's competing offering would have, but the tools ultimately would serve the same purpose: providing employers analytics about employees.[264]

In contrast, Facebook maintains a dedicated page of terms pertaining only to facial recognition. Specifically, Facebook represents, "We don't share your [face] template with anyone else but you. We don't have any face recognition features that tell strangers who you are."[265] These assurances are unsurprising. As the *New York Times* exposé notes, "technology that readily identifies everyone based on his or her face has been taboo because of its radical erosion of privacy. Tech companies capable of releasing such a tool have refrained from doing so . . . ."[266] This fact differentiates Clearview from hiQ: Whereas the latter sought to use LinkedIn's data to provide an analytics service that might have competed with LinkedIn's own, Clearview allegedly scraped Facebook images for a "taboo" purpose that Facebook and similarly-situated companies had not pursued.

4. California's Public Policy Is to Prevent Biometric Privacy Harms

The California Supreme Court weighs the potential of civil liability to deter future harm when determining whether to impose a novel tort duty.[267] In a scenario like Clearview, a limited duty in this context is indispensable to prevent future harm and is not inconsistent with the solicitude for biometric privacy expressed in California's recent omnibus privacy statute.[268] The "trust your overlords" problem is a

---

[263] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 998 (9th Cir. 2019).

[264] *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1106 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019) ("LinkedIn also points to specific user complaints it has received objecting to the use of data by third parties. In particular, two users complained that information that they had *previously* featured on their profile, but subsequently removed, remained viewable via third parties [other than hiQ].").

[265] *What Is the Face Recognition Setting on Facebook and How Does It Work?*, *supra* note 217.

[266] Hill, *supra* note 1.

[267] Christensen v. Superior Court, 820 P.2d 181, 198 (Cal. 1991).

[268] The California Consumer Privacy Act (CCPA), which became effective January 1, 2020, significantly changed the state's privacy laws. The CCPA is largely enforced by the California Attorney General, who is empowered to pursue statutory penalties for violations. *See* CAL. CIV. CODE § 1798.155(b) (West 2020). The Act does, however, provide a single private right of action, limited to data breaches. *Id.* § 150(a)(1). Substantively, the CCPA gives consumers rights to certain disclosures and deletions of personal information about them that businesses have collected. *Id.* §§ 100(a), 105(a). The Act expressly includes facial recognition templates as covered "biometric information" and provides that biometric information derived without subjects' consent is covered "personal information," and not uncovered "publicly available" information. §§ 140(b), (o)(2). The CCPA's scope remains uncertain, and a partner at a major law firm referred

problem in its own right, but it is an utterly intractable problem if one cannot even trust one's overlords!

C. Bad Faith Breaches of Contractual Duties Can Be Tortious

The preceding sub-Section argued that platform users could be owed duties by parties who accept a platform's terms. This sub-Section argues that a breach of such a duty that impinges upon a privacy interest may permit a plaintiff to recover from a party with whom it is in indirect privity. Ordinarily, breaches of contract do not permit recovery for emotional harm or other tortious damages.[269] But courts have permitted recovery for such damages in certain classes of contracts. The clearest example is the judge-made "tort of bad faith" in first- and third-party insurance claims.[270] In effect, courts in the mid-twentieth century recognized that insurance contracts "occupy a unique institutional role in any modern, capitalistic society" and modified contract rules to protect parties whose emotional well-being depended on these contracts.[271]

The tort of bad faith arose in response to a misalignment of incentives that threatened to undermine the modern architecture of liability insurance. Under a liability insurance contract, insurers agree to handle the legal defense of the insured and to pay claims directly to third-party claimants, up to the limits set forth in the insured's policy. If in the course of that litigation, the claimant offers to settle within the limits of the insured's policy, the incentives of the insurer and the insured diverge. The insurer is incentivized to take the case to trial: if it prevails against the claimant at trial, it pays nothing. If the insurer loses at trial, its liability is limited to the policy's limit. The insured, in contrast, only stands to lose if the insurer refuses a settlement offer within the policy limits, because it is he who will bear the costs of any excess liability assigned at trial.[272] In the words of a leading article on the bad faith tort, the insurer is "gambl[ing] with the insured's money . . . ."[273] Crucially, recovery for bad faith breach is not limited to contractual damages. Rather, the cause

to it as "the worst-drafted law he's worked with in over 30 years of practice . . ." Stewart Baker, *The Cyberlaw Podcast: Is CCPA Short for "Law of Unintended Consequences"?*, LAWFARE (Jan. 23, 2020), https://www.lawfareblog.com/cyberlaw-podcast-ccpa-short-law-unintended-consequences. A discussion of whether the CCPA could provide remedies similar to those argued for in this Article, or whether the CCPA might be interpreted to express a public policy disfavoring the private cause of action this Article proposes, would be premature and beyond this Article's scope.

[269] *See, e.g.*, Allen v. Jones, 104 Cal. App. 3d 207, 213 (1980).

[270] *See generally* Roger C. Henderson, *The Tort of Bad Faith in First-Party Insurance Transactions: Refining the Standard of Culpability and Reformulating the Remedies by Statute*, 26 U. MICH. J. L. REFORM 1 (1992).

[271] *Id.* at 7–8, 25–26.

[272] *Id.* at 20.

[273] *Id.* at 21.

of action sounds in tort, and plaintiffs may also recover for emotional harms stemming from the bad faith breach itself.[274]

The California Supreme Court pioneered the tort of bad faith in a series of three decisions known as the "California trilogy," the first two of which bear most directly on this Article's proposal.[275] The first case, *Comunale v. Traders & General Insurance Company*, held a liability insurer liable for the full amount of an adverse judgment because the insurer wrongfully refused to defend its insured.[276] The second, *Crisci v. Security Insurance Company of New Haven*, permitted an insured to collect damages for emotional distress attributable to her insurer's bad faith refusal of a settlement offer that left the insured exposed to a verdict that exceeded her policy limits.[277] Today, courts in most jurisdictions recognize some form of a bad faith claim in the insurance context.[278]

The proliferation of the bad faith tort tested its underlying doctrinal basis. Courts vacillated between describing it as a contractual or tort duty, measured by an intentionality or a negligence standard.[279] In a move reminiscent of modern-day information fiduciary proposals, courts also flirted with characterizing the insurer as a fiduciary.[280]

The California Supreme Court grew eager to prevent the unlimited expansion of the tort of bad faith. In 1995's *Freeman & Mills v. Belcher*, the Court overruled a 1984 decision that had recognized a tort claim for bad faith denial of a contract's existence.[281] The contract at issue in *Freeman & Mills* was "essentially a billing dispute between two commercial entities."[282] Accordingly, the Court's opinion focused on dispelling a theory of tort liability for bad faith breaches of "ordinary" commercial contracts.[283] To avoid such an outcome, *Freeman & Mills* propounded "a general rule precluding tort recovery for noninsurance contract breach, at least in the absence of violation of an independent duty arising from principles of tort law other

---

[274] Crisci v. Sec. Ins. Co. of New Haven, 426 P.2d 173, 179 (Cal. 1967).

[275] *See* Brent W. Brougher, Helen K. Michael & Brian Epps, *Insurance Bad Faith Law*, Westlaw Practical Law Practice Note 4-505-9149 (database updated May 6, 2011).

[276] Comunale v. Traders & Gen. Ins., 328 P.2d 198, 201–02 (Cal. 1958).

[277] *Crisci*, 426 P.2d at 179.

[278] *See* Brougher et al., *supra* note 275.

[279] Henderson, *supra* note 270, at 36–37.

[280] *See* Farmers Grp., Inc. v. Trimble, 691 P.2d 1138, 1142 (Colo. 1984) (describing "the quasi-fiduciary nature of the insurance relationship"); Henderson, *supra* note 270, at 35–36. *But see* Glenn v. Fleming, 799 P.2d 79, 89 (Kan. 1990) ("Breach of fiduciary duty is a tort; however, we have not recognized this tort in a bad faith and negligent defense action against an insurer."); *see also supra* text accompanying note 218 (discussing information fiduciary proposals).

[281] *See* Freeman & Mills, Inc. v. Belcher Oil Co., 900 P.2d 669, 670 (Cal. 1995).

[282] *Id.* at 689 (Mosk, J., concurring in part and dissenting in part).

[283] *Id.* at 672.

than the bad faith denial of the existence of, or liability under, the breached contract."[284]

Freeman & Mills represents a warranted hesitation to expand the bad faith tort to encompass all sorts of ordinary contracts. But its carveout for violations of independent tort duties means that it is not incompatible with a limited cause of action for individuals aggrieved by Clearview's alleged violations of terms of service. As Justice Mosk noted separately,

> this "independent duty arising from tort law" can originate from torts other than those traditionally recognized at common law. There are some types of intentionally tortious behavior unique to the contractual setting that do not fit into conventional tort categories. Allowing for the possibility of tort causes of action outside conventional categories is consistent with the malleable and continuously evolving nature of the tort law. . . .
>
> [A] tortious breach of contract outside the insurance context may be found when . . . one party intentionally breaches the contract intending or knowing that such a breach will cause severe, unmitigatable harm in the form of mental anguish, personal hardship, or substantial consequential damages.[285]

Four years later, a majority of the California Supreme Court cited Justice Mosk's *Freeman & Mills* opinion with approval and confirmed that intentional breaches known to cause severe mental anguish can be tortious even "outside the insurance context."[286] Other jurisdictions have acknowledged a similar possibility.[287]

Thus, the doctrine underlying the tort of bad faith supports a tort claim against entities that willfully breach material covenants in websites' terms of service, and in so doing injure the users of those sites. Not unlike insurance contracts, terms of service are fixtures of modern life that structure our behavior and our expectations. The prudent pedestrian would approach a crosswalk very differently if he could not

---

[284] *Id.* at 679–80 (internal citations omitted).

[285] *Id.* at 681 (Mosk, J., concurring in part and dissenting in part).

[286] Erlich v. Menezes, 981 P.2d 978, 984 (Cal. 1999).

[287] *See* Rawlings v. Apodaca, 726 P.2d 565, 576 (Ariz. 1986) ("[I]n special contractual relationships, when one party intentionally breaches the implied covenant of good faith and fair dealing, and when contract remedies serve only to encourage such conduct, it is appropriate to permit the damaged party to maintain an action in tort and to recover tort damages."). *But cf.* Francis v. Lee Enters., Inc., 971 P.2d 707, 710 (Haw. 1999) (quoting Dold v. Outrigger Hotel, 501 P.2d 368, 372 (Haw. 1972)) (abrogating a prior decision that had permitted tort actions where contracts are breached "in a wanton or reckless manner" and instead holding that the availability of tortious damages depends on the nature of the contract, rather than the manner of the breach). *See also* Landwehr v. Citizens Tr. Co., 329 N.W.2d 411, 413 (Wis. 1983) (discussing "continuing confusion in the law as to how to treat cases in which it is alleged that a contract has been performed improperly" and observing that the "substantive question of whether a breach of contract is actionable in tort" is "ordinarily . . . not significant" except when different limitations periods apply).

rely on motorists to hold liability insurance, or if a motorist's insurer could refuse to process his liability claim in bad faith. The pervasiveness of terms of service may also put actors on notice that certain intentional breaches can cause the "severe . . . mental anguish" that Justice Mosk identified as a hallmark of tortious breaches of contract.[288] For substantially the same reasons as the bad faith tort originated, then, courts can recognize that certain bad faith, willful breaches of terms of service can give rise to tortious damages.

D. Synthesizing Duties to Third Parties and Tortious Breaches: The Tort of Bad Faith Breach of Terms of Service

The preceding sub-Sections of Section V set forth the doctrinal support for two propositions: that certain contracts can give rise to duties to nonparties, and that breaches of certain contracts can give rise to tortious damages. This Section synthesizes these strains of California jurisprudence to propose a narrow new tort. The proposed cause of action bridges the gap between two interdependent parties to different instantiations of the same contractual terms. In effect, it would allow a platform user harmed by a third party's willful breach of that platform's terms of service to bring a suit for a privacy injury. In other words, it is a cause of action that gives Internet users the redress against Clearview that they currently lack, and it offers this redress for the right doctrinal and theoretical reasons. Because the tort constitutes an independent wrong, it could be interpreted to provide plaintiffs with a choice between damages for a privacy harm or a remedy in restitution that derives from a defendant's profits.[289]

Proposed language for the tort appears below:

---

[288] *Freeman & Mills, Inc.*, 900 P.2d at 681 (Mosk, J., concurring in part and dissenting in part).

[289] Pleading and proof requirements as to privacy damages may be relatively accommodating towards plaintiffs, and plaintiffs may be permitted to recover nominal damages. *See* RESTATEMENT (SECOND) OF TORTS: STRICT LIABILITY § 652H, Reporter's Note (AM. LAW INST. 1977); Fairfield v. Am. Photocopy Equip. Co., 291 P.2d 194, 198 (Cal. Dist. Ct. App. 1955); *see also, e.g.*, Snakenberg v. Hartford Cas. Ins. Co., 383 S.E.2d 2, 6 (S.C. Ct. App. 1989) (proving elements of intrusion into private affairs establishes damages as a matter of law), *cited with approval in* Rohrbaugh v. Wal-Mart Stores, Inc., 572 S.E.2d 881, 887 (W. Va. 2002). For the possibility of a restitutionary remedy for a privacy tort, *see* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 44 cmt. b (AM. LAW INST. 2011) ("Profitable interference with other protected interests, such as the claimant's right of privacy, gives rise to a claim under § 44 if the benefit to the defendant is susceptible of measurement"); *see also supra* text accompanying note 195.

> An actor who willfully breaches a covenant with a second party is liable to a third party for an invasion of privacy caused by the actor's willful breach if:
>
> (a) the actor knows or recklessly disregards the possibility that the breached covenant is material to a contractual relationship between the second party and the third party that existed at the time of the actor's breach, and
>
> (b) the actor knows or recklessly disregards the possibility that its breach of that covenant is likely to be highly offensive to that third party.

The tort is deliberately narrow. To ensure it covers only those situations "when the breach of contract is intentional and in bad faith, *and* is aggravated by certain particularly egregious forms of intentionally injurious activity,"[290] it contains three essential limitations: a willful breach of a covenant, recklessness to or knowledge of a tendency for that breach to harm a third party, and a materiality requirement for the breached covenant.

1. Willfulness of Breach

"Willfulness," for the purposes of the tort of bad faith breach of terms of service, requires a showing that contract "law imposed a duty on the defendant, that the defendant knew of this duty, and that he voluntarily and intentionally violated that duty."[291] The requirement of willful breach of duty eliminates the possibility that a defendant would be held liable simply for overlooking a provision of a lengthy terms of service agreement. Indeed, the tort requires a showing that the defendant was aware of a particular covenant *and* that it violated the covenant knowingly. As Justice Mosk observes, "the imposition of tort remedies for certain intentional breaches of contract serves to punish and deter business practices that constitute distinct social wrongs independent of the breach."[292] A willfulness requirement limits the proposed tort to only the most morally blameworthy behaviors.

2. Recklessness to or Knowledge of Consequences

Requiring defendants to be at least reckless as to the harms they cause further ensures that only blameworthy conduct will trigger liability under this tort. A meaningful intentionality requirement guards against the boundary-definition issues the tort of bad faith has encountered in the insurance context, where diverging interpretations have suggested both an intentionality requirement and a negligence threshold.[293] Clearview's actions give ample ground to impute knowledge of the harm its product might cause. The CEO did business under a pseudonym and, ap-

---

[290] *Freeman & Mills, Inc.*, 900 P.2d at 681 (Mosk, J., concurring in part and dissenting in part).

[291] *See* Cheek v. United States, 498 U.S. 192, 201 (1991) (defining willful *mens rea*).

[292] *Freeman & Mills, Inc.*, 900 P.2d at 683 (Mosk, J., concurring in part and dissenting in part).

[293] Henderson, *supra* note 270, at 36.

parently, took active measures to undermine public reporting on his company's service.[294] Moreover, once Clearview had attracted public attention, the CEO represented that the product was "strictly for law enforcement," even though subsequent reporting documented Clearview's business relationships with private companies.[295]

3. Materiality of Breached Covenant

Obviously, not all willful breaches of terms of service should be tortious, *even if* the breaching party acts with knowledge of harms that might result. So, what differentiates a bad faith breach of a covenant not to scrape for facial recognition purposes from, say, a bad faith breach of a covenant to behave civilly? The tort's materiality requirement filters out breaches that, while perhaps indecorous, are not so grave as to warrant tort liability. A court can use several factors to assess when a particular covenant is likely to be material to a user's relationship with a platform.

First, a court should evaluate the procedures and remedies available on the platform to address violations of that covenant. If such procedures exist, and empower individual users to act directly, this fact already weighs against tort liability. The presence of such mechanisms suggests, for example, that behavior that violates platforms' "community standards" would be unlikely to implicate this proposed tort. Facebook, Twitter, Google, and similar platforms all offer mechanisms for reporting abusive behavior.[296]

Second, a court should consider representations by a platform. The more explicitly a platform assures its users that it will not take a particular action, and the more the evidence suggests that such assurances affect users' decisions to use or not use the platform, the more likely that a third-party breach of such a covenant should be actionable. Recall that Facebook explicitly assures users, "We don't share your template with anyone else but you. We don't have any face recognition features that tell strangers who you are."[297] The more these representations suggest that a practice is "taboo" to mainstream enterprises[298]—like facial-recognition-for-hire—the more they should weigh in favor of tort liability for a willfully breaching party.

Third, a court should assess the plaintiff's expectations and the reasonableness of those expectations. This factor interlocks with the previous factors: if a platform makes representations to a user about how that user's data may be used, it is more

---

[294] Hill, *supra* note 1.

[295] Mac et al., *supra* note 1; Hill, *supra* note 1.

[296] *How to Report Things on Facebook*, FACEBOOK, https://www.facebook.com/help/181495968648557 (last visited Jan 27, 2021); *Report Violations*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-report-violation (last visited Jan. 27, 2021); *Other Reporting Options*, YOUTUBE, https://support.google.com/youtube/answer/2802057?hl=en (last visited Jan. 27, 2021).

[297] *What Is the Face Recognition Setting on Facebook and How Does It Work?*, *supra* note 217.

[298] Hill, *supra* note 1.

likely to influence that user's reasonable expectations about use. But a user's reasonable expectations about data use may also derive from implications in platforms' terms and affordances. That is, if a platform prohibits harassment and offers features to block and report harassers, it is not reasonable for a user to expect never to be harassed by another user on the platform.

Materiality is, admittedly, a somewhat protean and fact-specific requirement. But it is easy to ascertain in the sorts of outrageous, willful breaches that are properly subject to this proposed tort, because outrage over a violated covenant is likely to correlate to the materiality of that covenant. By applying the factors set forth above, courts can establish a bulwark against abuse of the tort of bad faith breach of terms of service.

E. Answering Some Threshold Objections

1. The Tort is Unlimited

The most obvious objection to this proposed tort is its potential boundlessness. Internet platforms' terms of service contain a whole lot of covenants, and it would obviously be untenable to let users enforce all of them against one another. The best illustrations of the potential problem are the community standards that platforms purportedly impose on users.[299] Mike Masnick has observed, "Content moderation at scale is impossible to do well. More specifically, it will always end up frustrating very large segments of the population and will always fail to accurately represent the 'proper' level of moderation of anyone."[300] Could a Twitter user, aggrieved that a fellow user appears to have violated Twitter's prohibition on "harassment," take action against the harasser directly, pursuant to the covenants in Twitter's rules?[301] The answer has to be "no," of course—but unless that "no" is principled, this Article's proposal isn't credible.

The most obvious rejoinder is the previous sub-Section's argument that the tort's three requirements of willful breach, knowledge or recklessness as to likelihood of harm, and materiality of the breached covenant ensure that inconsequential breaches will not give rise to tort liability. Also instructive is comparing the tort with a proposed duty that the California Supreme Court refused to recognize. In *Bily v. Arthur Young & Co.*, the California Supreme Court considered whether accountants could be held liable to third parties for negligent or intentional misrepresentations

[299] *See, e.g.*, *The Twitter Rules*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-rules (last visited Jan. 27, 2021).

[300] Mike Masnick, *Masnick's Impossibility Theorem: Content Moderation at Scale Is Impossible to Do Well*, TECHDIRT (Nov. 20, 2019, 9:31 AM), https://www.techdirt.com/articles/20191111/23032743367/masnicks-impossibility-theorem-content-moderation-scale-is-impossible-to-do-well.shtml.

[301] *The Twitter Rules*, *supra* note 299.

in the preparation of audit reports.[302] While *Bily* held that auditors *could* be liable for intentional misrepresentations, it declined to hold that accountants assumed a general duty to third parties who might rely on audits.[303] As summarized in a 2016 decision that applied both *Biakanja* and *Bily*, *Bily* emphasized three factors: (1) the possibility of "vast numbers of suits and limitless financial liability far out of proportion to its fault[,]" (2) the sophistication of the plaintiffs and their ability to "control and adjust their risks by contract rather than rely on tort liability[,]" and (3) "an increase in the cost and decrease in the availability of" the contracts that would include the novel duty.[304] Clearview differs from *Bily* on all three factors.

First, *Bily* treated it as significant that reliance on an erroneous audit was not the "sine qua non" of the plaintiff's ill-fated investments.[305] In contrast, Clearview's alleged conduct *is* the sine qua non of the plaintiffs' alleged injuries. Its conduct is not merely "close[ly] connect[ed]" to the plaintiffs' injury, it is *constitutive of* plaintiffs' injury. As the California Supreme Court observed, "moral force of the argument against unlimited liability . . . and the uncertain connection between [plaintiffs' injuries and defendants' conduct] pale as policy factors when intentional misconduct is in issue."[306] Liability for intentional conduct like Clearview's poses a far smaller risk of disproportionate liability than liability for mere negligence would have in *Bily*.

Second, if anything, the relative lack of sophistication of ordinary Internet users weighs in favor of tort liability. Unlike investors undertaking due diligence, who may have the resources, the sophistication, and the incentives to insulate themselves with *ex ante* contractual protections, ordinary platform users have minimal resources, low sophistication, and no ability to discourage third parties from breaching platforms' terms in deleterious ways. The fundamental dynamics of the "trust your overlords" problem mean that platform users are, on balance, worse equipped to take advance precautions than the plaintiffs were in *Bily*.

Third, and finally, *Bily*'s concern about how a novel tort duty might affect the availability of professional services has no good parallel in the Clearview facts. In *Bily*, the party that would have been subject to a new duty was the party offering the accounting services in question. In contrast, this Article's proposed tort places no new duties on platforms themselves. Rather, it recognizes a duty precisely in order to eliminate a class of services that should not have existed in the first place: nonconsensual, surreptitious, industrial-scale facial recognition.

---

[302] Bily v. Arthur Young & Co., 834 P.2d 745, 746–47 (Cal. 1992).

[303] *Id.* at 747.

[304] Centinela Freeman Emergency Med. Assocs. v. Health Net of California, Inc., 382 P.3d 1116, 1130 (Cal. 2016).

[305] *Bily*, 834 P.2d at 763.

[306] *Id.* at 773.

2. The Tort is Too Limited

The previous Section's reassurances about the tort's limited scope may have proved too much. Can this proposed tort do any work at all? Well, it can certainly offer plaintiffs redress against Clearview AI and numerous other bad actors. The Introduction informed readers that Clearview was not an innovator of facial recognition algorithms nor an innovator in building platforms for licensed data collection. But Clearview did not even originate its strategy of brazen scraping. In the 2020 headlines, Clearview may be touted as "The Secretive Company That Might End Privacy as We Know It," but in 2016, an app called FindFace was the "New Facial Recognition App [That] Could End Anonymity."[307] FindFace worked like Clearview, except that FindFace offered its functionality to the general public and it used photos from the Russian social network VKontakte instead of Facebook.[308] One of the more infamous uses of the Russian app FindFace was a message board's campaign to identify Russian women who appear in pornography or offer escort services, cross-reference their images with social media profiles, and harass the women and their acquaintances.[309]

Thus, even if the only conduct this Article's proposed tort could regulate were scraping for facial recognition, the tort applies to more than just a single, real-life defendant. But as our lives continue to grow around the pervasive influence of terms of service, other tortious breaches of those terms will surely become evident. It is true, however, that the narrowness of this tort reflects a narrowness that others have recognized more generally in conceptions of privacy that derive from contractual terms. As Eugene Volokh concedes, a contractual model of privacy "only lets people restrict speech by parties with whom they have a speech-restricting contract, express or implied."[310] Indeed, a third party who uncovers information obtained in confidence "simply hasn't agreed to anything that would waive its First Amendment rights" such that it could be prevented from disclosing.[311] Limiting the tort to violations of covenants that actors have agreed to is just that: a limitation. A narrow new tort would indeed offer meaningful redress for some aggrieved plaintiffs, but it

---

[307] Jonathan Frankle, *How Russia's New Facial Recognition App Could End Anonymity*, ATLANTIC (May 23, 2016), https://www.theatlantic.com/technology/archive/2016/05/findface/483962/; Hill, *supra* note 1.

[308] Janus Kopfstein, *Twitter Bans Russian Face Recognition App Used to Harass Porn Stars*, VOCATIV (Dec. 16, 2016, 12:15 PM), https://www.vocativ.com/384720/twitter-russian-face-recognition-porn-stars/ (describing FindFace's data source as scraping).

[309] Kevin Rothrock, *Facial Recognition Service Becomes a Weapon Against Russian Porn Actresses*, GLOBAL VOICES ADVOC. (Apr. 22, 2016), https://advox.globalvoices.org/2016/04/22/facial-recognition-service-becomes-a-weapon-against-russian-porn-actresses/.

[310] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1061 (2000).

[311] *Id.*

cannot establish the comprehensive changes that proponents of information fiduciaries or market regulation have advocated.

There is another reason for this proposal's limited reach: it has endeavored to craft an accurate theory of harm, and a suitable route to redress, using accepted doctrinal forms. It might be more straightforward to anchor the harm in individuals' attestations that they feel outraged by facial recognition. Instead of citing that outrage directly, this Article invokes the limited forms of popular objection to facial recognition that end up codified in platforms' terms of service. Finding harm in the willful breach of a covenant, rather than the provocation of outrage *per se*, means that the proposal will not capture every scenario in which people perceive themselves to be victimized. But a focus on form can also give tighter explanations for why particular conduct is objectionable, and suggestions for redress that are easier to implement.

3. What About the First Amendment?

There are plenty of reasons that actors good and bad, commercial and noncommercial, might engage in scraping. Journalists and researchers scrape websites to collect data for study and reportage.[312] Popular benchmarks for academic research in facial recognition derive from large-scale web scraping.[313] I personally used scraping software to conduct research and archive materials for this Article.[314] Courts are beginning to take note of scraping's significant role in modern public discourse. A federal district court observed in 2018 that scraping as a method of information-gathering "plausibly falls within the ambit of the First Amendment."[315] And Clearview itself asserts that its scraping activities are fully protected by the First Amendment.[316]

Balancing the constitutional safeguards for these different speech interests against the various forms of criminal and civil liability that scraping might trigger is beyond the scope of this Article. Scholars who have proposed more sweeping legal innovations to rectify online privacy harms have also had to address more sweeping First Amendment objections to their proposals.[317] Fortunately, the modesty of this

---

[312] Letter from Jameel Jaffer, Exec. Dir., Knight First Amend. Inst., to Mark Zuckerberg, CEO, Facebook (Aug. 6, 2018), https://s3.amazonaws.com/kfai-documents/documents/d6ebc73dd9/Facebook_Letter.pdf; *see also* Sandvig v. Sessions, 315 F. Supp. 3d 1, 15–16 (D.D.C. 2018) (discussing research interests in scraping).

[313] Madhumita Murgia & Max Harlow, *Who's Using Your Face? The Ugly Truth About Facial Recognition*, FIN. TIMES (Sept. 18, 2019), https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e.

[314] *See Your Personal Research Assistant*, ZOTERO, https://www.zotero.org/ (last visited Jan. 27, 2021).

[315] *Sandvig*, 315 F. Supp. 3d at 15–16.

[316] *See* CBS News, *supra* note 261, at 7:00.

[317] *See* Zahra Takhshid, *Retrievable Images on Social Media Platforms: A Call for a New*

Article's proposal diminishes the chances that its proposed tort would conflict with the First Amendment. This Section briefly addresses why this Article's proposal creates minimal First Amendment friction.

The tort of bad faith breach of terms of service is relatively unlikely to conflict with the First Amendment because courts are quite deferential to limitations on speech imposed by contracts between private parties. Eugene Volokh has observed that speech restrictions enforced pursuant to express or implied contracts are "eminently defensible under existing free speech doctrine."[318] This Article's proposed tort simply provides that a duty that a defendant had assumed in relation to an online platform is also owed, impliedly and in narrow circumstances, to users of that platform. Thus, the tort's compatibility with the First Amendment correlates to anti-scraping covenants' compatibility with the First Amendment.[319]

There is some reason to believe that scraping prohibitions in terms of service, at least as applied to actors like Clearview, may not conflict with the First Amendment. A First Amendment violation cannot occur without "state action."[320] Some courts have held that judicial enforcement of speech-restrictive covenants between private parties is not state action at all.[321] In *Cohen v. Cowles Media Company*, the Supreme Court acknowledged that a promissory estoppel claim against a reporter who revealed a source after promising not to would constitute state action, but that such state action would be constitutional.[322] And appellate courts have even upheld tort actions for trespass and breach of a duty of loyalty against *newsgatherers* who procured information through forbidden means.[323]

Privacy Tort, 68 BUFF. L. REV. 139, 148 (2020) (addressing First Amendment objections to a proposed new privacy tort).

[318] Volokh, *supra* note 310, at 1057.

[319] However, non-contractual suits may draw constitutional scrutiny that strictly contractual suits may not. *See* Cohen v. Cowles Media Co., 501 U.S. 663, 668 (1991) ("The initial question we face is whether a private cause of action for promissory estoppel involves 'state action' within the meaning of the Fourteenth Amendment such that the protections of the First Amendment are triggered. . . . In this case, the Minnesota Supreme Court held that if Cohen could recover at all it would be on the theory of promissory estoppel, a state-law doctrine which, in the absence of a contract, creates obligations never explicitly assumed by the parties. These legal obligations would be enforced through the official power of the Minnesota courts. Under our cases, that is enough to constitute 'state action' for purposes of the Fourteenth Amendment.").

[320] *See* Cent. Hardware Co. v. Nat'l Labor Relations Bd., 407 U.S. 539, 547 (1972).

[321] *See* Merrell v. Renier, No. C06-404JLR, 2006 WL 3337368, at *8 (W.D. Wash. Nov. 16, 2006) (listing cases).

[322] *Cohen*, 501 U.S. at 668, 671–72.

[323] *See* Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505, 521 (4th Cir. 1999); *see also* Desnick v. Am. Broad. Companies, Inc., 44 F.3d 1345, 1355 (7th Cir. 1995) (Posner, C.J.) (dismissing privacy, trespass, and fraud claims brought by medical practitioners depicted in a television broadcast, but explicitly noting the potential viability of a breach of contract claim that the plaintiffs had voluntarily dismissed).

Of course, courts remain free to find formal defects in terms of service *qua* contracts, or to conclude that anti-scraping covenants are otherwise unenforceable. But such conclusions would not just undermine this Article's proposed tort. Judicial repudiation of the form or the substance of online platforms' terms of service would disturb many more established areas of law and enterprise. More significant revisions of private ordering online may indeed be necessary to address fully the privacy harms this Article chronicles. The point is not that this Article's proposal can or should endure radical changes in jurisprudence, but rather that its proposed tort can serve as a stopgap in lieu of more comprehensive changes to our online information ecosystem.

VI. CONCLUSION

The Clearview facial recognition scandal is a monumental breach of privacy, and it came to light just months after the Ninth Circuit narrowed the law that seemed to offer the clearest route to redress. Section II argued that the Ninth Circuit's *hiQ* decision marks, at least for the time being, the reascension of common law causes of action in a field that had been dominated by the CFAA. Section III showed that the tangle of possible common law theories that courts must now adapt to cyberspace resembles the strained property and contract formalism that privacy scholars and plaintiffs reckoned with at the turn of the twentieth century. It suggested that modern courts, following the example some of their predecessors set over a century ago, may properly recognize some common law remedies for present-day misconduct. Section IV catalogued familiar common law claims to argue that no established property, tort, or contract claim fully captures the harm that conduct like Clearview's alleged behavior wreaks on individual Internet users. Section V proposed a new tort that can provide aggrieved plaintiffs with a proper remedy without sacrificing doctrinal fidelity or theoretical coherence.

The proposed tort would allow users of an Internet platform to sue third parties who cause them harm by willfully breaching certain material covenants in that platform's terms of service. This tort is not a panacea. It does not alter the systemic characteristics that contribute to an extractive and inequitable social media marketplace. It will offer relief only on narrow sets of facts. And, much like the ordinary Internet users who must "trust their overlords" to police harmful behavior on their platforms, the tort's viability depends in large part on the scruples of dominant Internet enterprises.

But this proposal's limitations are also its strengths. Its modest scope and precedential grounding make it less likely to succumb to constitutional challenges or a sclerotic political process. Unlike more sweeping interventions, this Article's proposed tort is within a court's power to recognize. Indeed, the proposal flows from two established common law doctrines: the recognition that the special character of certain bilateral contracts can engender duties to third parties, and the recognition

that certain contracts are so socially significant that their bad faith breach gives rise to tortious damages. This proposal will not shift the paradigm of commercial social media. But so long as that paradigm remains, this Article's proposal provides a stopgap to protect privacy interests until more systemic reforms take root.