INTERNET LAW: CASES & PROBLEMS

SPRING 2020 SUPPLEMENT

James Grimmelmann
Professor of Law
Cornell Tech and Cornell Law School

www.semaphorepress.com

Table of Contents

Copyright and Your Rights

Delete the Nonconsensual Pornography Problem in Section 3.C.9 at page 183. Insert the following case in section 3.C.5 at page 159, immediately before *Gawker Media v. Bollea*.

The following case includes discussion of nonconsensual pornography.

STATE V. AUSTIN

2019 IL 123910

Justice Neville delivered the judgment of the court, with opinion:

Defendant Bethany Austin was charged with violating section 11-23.5(b) of the Criminal Code of 2012 (720 ILCS 5/11-23.5(b)), which criminalizes the nonconsensual dissemination of private sexual images. ...

I. Background

Defendant was engaged to be married to Matthew, after the two had dated for more than seven years. Defendant and Matthew lived together along with her three children. Defendant shared an iCloud account with Matthew, and all data sent to or from Matthew's iPhone went to their shared iCloud account, which was connected to defendant's iPad. As a result, all text messages sent by or to Matthew's iPhone automatically were received on defendant's iPad. Matthew was aware of this data sharing arrangement but took no action to disable it.

While Matthew and defendant were engaged and living together, text messages between Matthew and the victim, who was a neighbor, appeared on defendant's iPad. Some of the text messages included nude photographs of the victim. Both Matthew and the victim were aware that defendant had received the pictures and text messages on her iPad. Three days later, Matthew and the victim again exchanged several text messages. The victim inquired, "Is this where you don't want to message [because] of her?" Matthew responded, "no, I'm fine. [S]omeone wants to sit and just keep watching want [*sic*] I'm doing I really do not care. I don't know why someone would wanna put themselves through that." The victim replied by texting, "I don't either. Soooooo baby ...."

Defendant and Matthew cancelled their wedding plans and subsequently broke up. Thereafter, Matthew began telling family and friends that their relationship had ended because defendant was crazy and no longer cooked or did household chores.

In response, defendant wrote a letter detailing her version of events. As support, she attached to the letter four of the naked pictures of the victim and copies of the text messages between the victim and Matthew. When Matthew's cousin received the letter along with the text messages and pictures, he informed Matthew.

Upon learning of the letter and its enclosures, Matthew contacted the police. The victim was interviewed during the ensuing investigation and stated that the pictures were private and only intended for Matthew to see. The victim acknowledged that she was aware that Matthew had shared an iCloud account with defendant, but she thought it had been deactivated when she sent him the nude photographs.

Defendant was charged by indictment with one count of nonconsensual dissemination of private sexual images. ...

II. Analysis ...

A. The Necessity for the Law

Section 11-23.5 addresses the problem of nonconsensual dissemination of private sexual images, which is colloquially referred to as "revenge porn." Generally, the crime involves images originally obtained without consent, such as by use of hidden cameras or victim coercion, and images originally obtained with consent, usually within the context of a private or confidential relationship. Once obtained, these images are subsequently distributed without consent. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn,* 49 Wake Forest L. Rev. 345, 346 (2014); see Adrienne N. Kitchen, *The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment,* 90 Chi.-Kent L. Rev. 247, 247-48 (2015).

The colloquial term "revenge porn" obscures the gist of the crime:

> "In essence, the crux of the definition of revenge porn lies in the fact that the victim did not consent to its *distribution*—though the victim may have consented to its recording or may have taken the photo or video themselves. As a result, the rise of revenge porn has (unsurprisingly) gone hand-in-hand with the increasing use of social media and the Internet, on which people constantly exchange ideas and images without asking permission from the originator." Christian Nisttáhuz, *Fifty States of Gray: A Comparative Analysis of 'Revenge-Porn"Legislation Throughout the United States and Texas's Relationship Privacy Act,* 50 Tex. Tech. L. Rev. 333, 337 (2018).

Indeed, the term "revenge porn," though commonly used, is misleading in two respects. First, "revenge" connotes personal vengeance. However, perpetrators may be motivated by a desire for profit, notoriety, entertainment, or for no specific reason at all. The only common factor is that they act without the consent of the person depicted. Second, "porn" misleadingly suggests that visual depictions of nudity or sexual activity are inherently pornographic. ...

This is a unique crime fueled by technology:

> "We do not live in a world where thousands of websites are devoted to revealing private medical records, credit card numbers, or even love letters. By contrast, `revenge porn' is featured in as many as 10,000 websites, in addition to being distributed without consent through social media, blogs, emails, and texts. There is a demand for private nude photos that is unlike the demand for any other form of private information. While nonconsensual pornography is not a new phenomenon, its prevalence, reach, and impact have increased in recent years in part because technology and social media make it possible to 'crowdsource' abuse, as well as make it possible for unscrupulous individuals to profit from it. Dedicated 'revenge porn' sites and other forums openly solicit private intimate images and expose them to millions of viewers, while allowing the posters themselves to hide in the shadows." Franks, *Revenge Porn" Reform: A View from the Front Lines*, 69 Fla. L. Rev. 1251, 1260-61 (2017).

Consent is contextual. "The consent to create and send a photo or the consent to be photographed by another is one act of consent that cannot be equated with consenting to distribute that photo to others outside of the private relationship... ." Erica Souza, *"For His Eyes Only": Why Federal Legislation Is Needed to Combat*

Revenge Porn, 23 UCLA Women's L.J. 101, 109-10 (2016). Accordingly, criminal liability here does not depend on "whether the image was initially obtained with the subject's consent; rather, it is the absence of consent to the image's distribution that renders the perpetrator in violation of the law." Ava Schein, Note, *When Sharing Is Not Caring: Creating an Effective Criminal Framework Free From Specific Intent Provisions to Better Achieve Justice for Victims of Revenge Pornography,* 40 Cardozo L. Rev. 1953, 1955-56 (2019). The nonconsensual dissemination of private sexual images "is not wrong because nudity is shameful or because the act of recording sexual activity is inherently immoral. It is wrong because exposing a person's body against her will fundamentally deprives that person of her right to privacy." Franks, *supra,* at 1260. ...

The overwhelming majority of state legislatures have enacted laws criminalizing the nonconsensual dissemination of private sexual images. ...

B. The General Assembly's Solution

Against this historical and societal backdrop, we consider the terms of the statutory provision at issue. Section 11-23.5(b) provides as follows:

> (b) A person commits non-consensual dissemination of private sexual images when he or she:
>
> (1) intentionally disseminates an image of another person:
>
> (A) who is at least 18 years of age; and
>
> (B) who is identifiable from the image itself or information displayed in connection with the image; and
>
> (C) who is engaged in a sexual act or whose intimate parts are exposed, in whole or in part; and
>
> (2) obtains the image under circumstances in which a reasonable person would know or understand that the image was to remain private; and
>
> (3) knows or should have known that the person in the image has not consented to the dissemination.

720 ILCS 5/11-23.5(b). ...

D. First Amendment ...

1. No Categorical Exception ...

We acknowledge, as did the Vermont Supreme Court, that the nonconsensual dissemination of private sexual images "seems to be a strong candidate for categorical exclusion from full First Amendment protections" based on "[t]he broad development across the country of invasion of privacy torts, and the longstanding historical pedigree of laws protecting the privacy of nonpublic figures with respect to matters of only private interest without any established First Amendment limitations." *State v. VanBuren,* 2018 VT 95, ¶ 43. However, we decline to identify a new categorical first amendment exception when the United States Supreme Court has not yet addressed the question. ...

2. Degree of Scrutiny ...

In contrast to content-based speech restrictions, regulations that are unrelated to the content of speech are subject to an intermediate level of scrutiny because in most cases they pose a less substantial risk of excising certain ideas or viewpoints from the public dialogue. We conclude that section 11-23.5(b) is subject to an intermediate level of scrutiny for two independent reasons. First, the statute is a

content-neutral time, place, and manner restriction. Second, the statute regulates a purely private matter.

a. Time, Place, and Manner ...

We recognize that section 11-23.5(b) on its face targets the dissemination of a specific category of speech—sexual images. However, the statute is content neutral. A regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others. ...

In the case at bar, section 11-23.5(b) is justified on the grounds of protecting privacy. Section 11-23.5(b) distinguishes the dissemination of a sexual image not based on the content of the image itself but, rather, based on whether the disseminator obtained the image under circumstances in which a reasonable person would know that the image was to remain private and knows or should have known that the person in the image has not consented to the dissemination. There is no criminal liability for the dissemination of the very same image obtained and distributed with consent. The *manner* of the image's acquisition and publication, and not its *content,* is thus crucial to the illegality of its dissemination. ...

Viewed as a privacy regulation, section 11-23.5 is similar to laws prohibiting the unauthorized disclosure of other forms of private information, such as medical records (410 ILCS 50/3(d) (West 2016)), biometric data (740 ILCS 14/15 (West 2016)), or Social Security numbers (5 ILCS 179/10 (West 2016)). The entire field of privacy law is based on the recognition that some types of information are more sensitive than others, the disclosure of which can and should be regulated. To invalidate section 11-23.5 would cast doubt on the constitutionality of these and other statutes that protect the privacy rights of Illinois residents. ...

b. Purely Private Matter ...

Speech on matters of public concern lies at the heart of first amendment protection. However, first amendment protections are less rigorous where matters of purely private significance are at issue ...

The Supreme Court has articulated some guiding factors:

> "Speech deals with matters of public concern when it can be fairly considered as relating to any matter of political, social, or other concern to the community, or when it is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public. The arguably inappropriate or controversial character of a statement is irrelevant to the question whether it deals with a matter of public concern."

Snyder v. Phelps, 562 U.S. 443, 453 (2011). ...

Applying these principles to the instant case, we have no difficulty in concluding that the nonconsensual dissemination of the victim's private sexual images was not an issue of public concern. Matthew was telling his and defendant's families and friends that it was defendant's fault that their relationship ended. Defendant responded with a letter, in which she explained her version of events. To this letter defendant attached the victim's private sexual images along with text messages between the victim and Matthew. The victim's private sexual images, in context with her and Matthew's text messages, were never in the public domain. They do not relate to any broad issue of interest to society at large. The message they convey is not a matter of public import. *Cf. id.* (holding that messages on protest signs

at a private funeral related to broad issues of interest to society at large and were matters of public import). Rather, the public has no legitimate interest in the private sexual activities of the victim or in the embarrassing facts revealed about her life. ...

3. Applying Intermediate Scrutiny ...

Generally, to survive intermediate scrutiny, the law must serve an important or substantial governmental interest unrelated to the suppression of free speech and must not burden substantially more speech than necessary to further that interest or, in other words, must be narrowly tailored to serve that interest without unnecessarily interfering with first amendment freedoms, which include allowing reasonable alternative avenues of communication. ...

[*Governmental interest*] In the case at bar, we conclude that section 11-23.5 serves a substantial government interest. [The court summarized the development of privacy laws, especially the tort of public disclosure of private facts.] ...

Specifically, the nonconsensual dissemination of private sexual images causes unique and significant harm to victims in several respects. Initially, this crime can engender domestic violence. Perpetrators threaten disclosure to prevent victims from ending relationships, reporting abuse, or obtaining custody of children. Sex traffickers and pimps threaten disclosure to trap unwilling individuals in the sex trade. Rapists record their sexual assaults to humiliate victims and deter them from reporting the attacks.

Also, the victims' private sexual images are disseminated with or in the context of identifying information. Victims are frequently harassed, solicited for sex, and even threatened with sexual assault and are fired from their jobs and lose future employment opportunities. Victims additionally suffer profound psychological harm. Victims often experience feelings of low self-esteem or worthlessness, anger, paranoia, depression, isolation, and thoughts of suicide.

Additionally, the nonconsensual dissemination of sexual images disproportionately affects women, who constitute 90% of the victims, while men are most commonly the perpetrators and consumers ....

[*Least restrictive means*] In contending that the statute fails strict scrutiny, defendant argues that a penal statute is not the least restrictive means to accomplish the alleged compelling government interest. ...

We conclude that the substantial government interest of protecting Illinois residents from nonconsensual dissemination of private sexual images would be achieved less effectively absent section 11-23.5. ...

Civil actions are inadequate. ...

> "Civil suits based on privacy violations are problematic. Most victims want the offensive material removed and civil suits almost never succeed in removing the images due to the sheer magnitude of dissemination. Highly publicized trials often end in re-victimization. Civil litigation is expensive and time-consuming, and many victims simply cannot afford it. It is difficult to identify and prove who the perpetrator is for legal proceedings because it is so easy to anonymously post and distribute revenge porn. Even when victims can prove who the perpetrator is in court and win money damages, many defendants are judgment-proof so victims cannot collect. ...
>
> Further, a court order requiring a defendant or website to remove the images would fail to remove the images from the web entirely, particularly as they appear on numerous sites. Because most

> perpetrators are judgment-proof, and injunctive relief may be difficult to obtain and would ultimately fail to remove the images, civil suits are poor remedies. As perpetrators frequently have nothing to lose, which is why they engage in this behavior in the first place, civil suits do not deter revenge porn."

Kitchen, *supra*, at 251-53. ...

[*Burdening more speech than necessary*] We next consider whether section 11-23.5 burdens substantially more speech than necessary. ...

Subsection (b) is narrowly tailored in several respects so as not to burden more speech than necessary. First, the images must be "private sexual images" that portray any of several specific features, including the depiction of a person whose intimate parts are exposed or visible, in whole or in part, or who is engaged in a sexual act as defined in the statute. *Id.* § 11-23.5(a), (b)(1)(C). Therefore, the scope of the statute is restricted to images that can fairly be characterized as being of a discreet and personal nature. ...

Second, the person portrayed in the image must be over the age of 18 and identifiable from the image or information displayed in connection with the image. 720 ILCS 5/11-23.5(b)(1)(A)-(B) (West 2016). The statute is inapplicable if the image does not contain sufficient information to identify the person depicted. Therefore, section 11-23.5(b) burdens only speech that targets a specific person.

Third, the image must have been obtained under circumstances in which a reasonable person would know or understand that it was to remain private. *Id.* § 11-23.5(b)(2). We construe this provision as requiring a reasonable awareness that privacy is intended by the person depicted. This requirement limits the statute's application to the types of personal, direct interactions or communications that are typically involved in a close or intimate relationship. Thus, this provision ensures that the statute is inapplicable if the image was obtained under circumstances where disclosure to another is a natural and expected outcome.

Fourth, the person who disseminates such an image must have known or should have known that the person portrayed in the image has not consented to the dissemination. 720 ILCS 5/11-23.5(b)(3) (West 2016). The lack of consent to dissemination forms the core of the statute and its protective purpose. As with the expectation of privacy discussed above, we construe this provision to incorporate a reasonable awareness of the lack of consent to dissemination. Where the person portrayed in the image has consented to its disclosure, the statute simply does not apply and poses no restriction on the distribution of the image to others.

Fifth, the statute specifically requires that the dissemination of private sexual images be intentional. *Id.* § 11-23.5(b)(1). Therefore, the probability that a person will inadvertently violate section 11-23.5(b) while engaging in otherwise protected speech is minimal.

Section 11-23.5 also includes several specific exemptions. Subsection (c) provides as follows:

> (c) The following activities are exempt from the provisions of this Section:
>
> (1) The intentional dissemination of an image of another identifiable person who is engaged in a sexual act or whose intimate parts are exposed when the dissemination is for the purpose of a criminal investigation that is otherwise lawful.
>
> (2) The intentional dissemination of an image of another identifiable person who is engaged in a sexual act or whose intimate parts are ex-

posed when the dissemination is made for the purpose of, or in connection with, the reporting of unlawful conduct.

(3) The intentional dissemination of an image of another identifiable person who is engaged in a sexual act or whose intimate parts are exposed when the images involve voluntary exposure in public or commercial settings.

(4) The intentional dissemination of an image of another identifiable person who is engaged in a sexual act or whose intimate parts are exposed when the dissemination serves a lawful public purpose.

Id. § 11-23.5(c).

These exemptions shield from criminal liability any dissemination of a private sexual image that advances the collective goals of ensuring a well-ordered system of justice and protecting society as a whole. In addition, subsection (c)(3) recognizes that public disclosure has been sanctioned based on the very nature of such an image. Finally, the statute does not apply to electronic communication companies that provide access to the Internet, public mobile services, or private radio services. *Id.* § 11-23.5(d).

Based on the statutory terms set forth above, section 11-23.5 is narrowly tailored to further the important governmental interest identified by the legislature. Accordingly, we conclude the statute does not burden substantially more speech than necessary.

Also, we observe that reasonable avenues of communication remain. Under section 11-23.5, "[p]eople remain free to produce, distribute, and consume a vast array of consensually disclosed sexually explicit images. Moreover, they remain free to criticize or complain about fellow citizens in ways that do not violate the privacy rights of others." Franks, *supra,* at 1326. ...

In this case, defendant makes no argument that her speech would have been in any way stifled by not attaching the victim's private sexual images to her letter. We hold that section 11-23.5 satisfies intermediate scrutiny.

E. First Amendment Overbreadth ...

As support of its overbreadth determination, the circuit court posited several hypothetical scenarios as examples of circumstances in which the statute would impermissibly restrict protected speech. ...

We ... reject the circuit court's suggestion that section 11-23.5(b) would impose criminal liability on a person who discovers and shares with other family members nude sketches of his or her grandmother that were created by his or her grandfather but were discovered in an attic after her death. ... Obviously, the statute is intended to protect living victims from the invasion of privacy and the potential threat to health and safety that is intrinsic in the disclosure of a private sexual image. ... In light of the fact that a deceased person cannot suffer the types of injuries that section 11-23.5(b) is intended to safeguard against, the statute does not apply to the hypothetical situation suggested by the circuit court.

The circuit court also questioned whether section 11-23.5(b) would criminalize the sharing of nude sketches of a person's grandmother if his or her grandfather had been an artist such as Andrew Wyeth, who created the "Helga Pictures" that remained secret for many years, or Pablo Picasso. ... Given that a model who poses for an artist is aware of that person's profession, it will generally be understood that the sketch or painting may be displayed to others at some point in time. In such a circumstance, the statute would not apply because a reasonable person

would not know or understand that the image was to remain private. The same is true of the circuit court's reference to images published in Playboy Magazine and in movies or programs depicting nudity. The people portrayed in such images have clearly consented to public disclosure and dissemination. Indeed, that is the whole point of appearing in such a photograph or film. ...

The circuit court further observed that section 11-23.5(b) does not expressly require a showing of any specific harm to the victim. ... [W]e believe that the unauthorized dissemination of a private sexual image, which by definition must depict a person while nude, seminude, or engaged in sexually explicit activity, is presumptively harmful.

In evaluating the competing social costs at stake, we have held that Illinois has a substantial governmental interest in protecting the privacy of persons who have not consented to the dissemination of their private sexual images. Although defendant claims that section 11-23.5(b) will deter the free speech of persons who have legally and unconditionally obtained the private sexual images of others, her assertion is unpersuasive given the limited application of the statute and the fact that any possible overbreadth is minor when considered in light of the statute's legitimate sweep. Defendant also contends that section 11-23.5 "criminalizes an adult complainant's own stupidity at the expense of the [f]irst [a]mendent." Yet this argument entirely disregards the victim's first amendment right to engage in a personal and private communication that includes a private sexual image. Defendant's crude attempt to "blame the victim" is not well received and reinforces the need for criminalization. Accordingly, defendant has not established that, on balance, the social costs weigh in her favor or that the marginal restraint on constitutionally protected speech is greater than necessary to advance the governmental interest at stake.

F. Constitutional Vagueness

Defendant also argues that section 11-23.5(b) is unconstitutionally vague on its face in violation of her right to due process (U.S. Const., amend. XIV; Ill. Const. 1970, art. I, § 2). ...

We are similarly unpersuaded by defendant's assertion that section 11-23.5 violates due process because a private sexual image that has been shared with another person is not a truly private matter. According to defendant, the "unconditional" disclosure of such an image imposes no duty on the recipient to keep the image private and operates to relinquish all privacy rights of the person depicted therein. ... [A]cceptance of defendant's argument would impose the strictures of a commercial transaction on personal and intimate communications by requiring that the person portrayed elicit an express promise from the recipient that the image will be kept private. ...

Justice Garman, dissenting:

Even though both parties agree a strict scrutiny analysis applies in this case, the majority concludes an intermediate level of scrutiny is the appropriate standard. I, however, would find the statute criminalizes the dissemination of images based on their content—"private sexual images"—and thus strict scrutiny applies. Moreover, in applying strict scrutiny, I would find the statute is neither narrowly tailored nor the least restrictive means of dealing with the nonconsensual dissemination of private sexual images. ...

Contrary to the majority's belief, the content of the image is precisely the focus of section 11-23.5. It is not a crime under this statute to disseminate a picture of a

fully clothed adult man or woman, even an unflattering image obtained by the offender under circumstances in which a reasonable person would know or understand the image was to remain private and he knows or should have known the person in the image had not consented to its dissemination. However, if the man or woman in the image is naked, the content of that photo makes it a possible crime. Thus, one must look at the content of the photo to determine whether it falls within the purview of the statute. ...

Assuming the State has a compelling interest in prohibiting nonconsensual dissemination of private sexual images, I would find the statute is not narrowly tailored to promote that interest. ...

Unlike those states that specifically require an intent to harm, harass, intimidate, threaten, coerce, embarrass, frighten, terrify, torment, terrorize, degrade, demean, annoy, alarm, or abuse the victim, the Illinois statute requires nothing of the sort. Although the majority finds the statute "implicitly includes an illicit motive or malicious purpose", the absence of any such nefarious intentions proscribed by other states opens the door wide for innocent conduct to be criminalized. ...

The Vermont statute also limited a violation to when the disclosure would cause a reasonable person to suffer harm, and it defines "harm" as "physical injury, financial injury, or serious emotional distress." Vt. Stat. Ann. tit. 13, § 2606(a)(2). Under the Illinois law, there is no objective or subjective harm requirement. *Cf.* N.D. Cent. Code § 12.1-17-07.2(2)(c) (2017) (requiring "[a]ctual emotional distress or harm" to the depicted individual as a result of the distribution of intimate images); Or. Rev. Stat. § 163.472(1)(c), (d) (2017) (requiring the victim to be "harassed, humiliated or injured by the disclosure" and that "[a] reasonable person would be harassed, humiliated or injured by the disclosure") [and four other states with similar requirements]. The majority, however, presumes the dissemination is harmful. Again, along with the absence of a malicious purpose, the lack of a showing of any specific harm to the alleged victim casts the net of criminality too far in my mind.

A hypothetical posed to the State during oral argument illustrates this point. Two people go out on a date, and one later sends the other a text message containing an unsolicited and unappreciated nude photo. The recipient then goes to a friend, shows the friend the photo, and says, "look what this person sent me." Has the recipient committed a felony? The State conceded that the recipient had, assuming the recipient knew or should have known that the photo was intended to remain a private communication.

The statute also does not provide the least restrictive means of dealing with the problem. The legislature could provide for a private right of action against an offender. It could also provide avenues of equitable relief, including temporary restraining orders, preliminary injunctions, or permanent injunctions. Instead, the statute criminalizes the conduct and subjects offenders to a possible term of one to three years in prison. ...

QUESTIONS

1. **Special-Purpose Laws**: Do you agree that there is a need for criminal statutes specifically directed at nonconsensual distribution of intimate images? Could Austin or Matthew have been prosecuted or sued for copyright infringement? For intentional infliction of emotional distress? Wiretapping? Public disclosure of private facts?

2. **Doctrinal Inflexibility**: Count the number of different First Amendment doctrines discussed by the court. Why is it so challenging to analyze the Illinois statute in terms of established caselaw?

Insert the following case in Section 5.C at page 341, immediately before the Line-Jump problem.

HIQ LABS, INC. V. LINKEDIN CORP.
938 F.3d 985 (9th Cir. 2019)

Berzon, Circuit Judge:

May LinkedIn, the professional networking website, prevent a competitor, hiQ, from collecting and using information that LinkedIn users have shared on their public profiles, available for viewing by anyone with a web browser? …

I.

Founded in 2002, LinkedIn is a professional networking website with over 500 million members. Members post resumes and job listings and build professional "connections" with other members. LinkedIn specifically disclaims ownership of the information users post to their personal profiles: according to LinkedIn's User Agreement, members own the content and information they submit or post to LinkedIn and grant LinkedIn only a non-exclusive license to "use, copy, modify, distribute, publish, and process" that information.

LinkedIn allows its members to choose among various privacy settings. Members can specify which portions of their profile are visible to the general public (that is, to both LinkedIn members and nonmembers), and which portions are visible only to direct connections, to the member's "network" (consisting of LinkedIn members within three degrees of connectivity), or to all LinkedIn members. This case deals only with profiles made visible to the general public. …

LinkedIn has taken steps to protect the data on its website from what it perceives as misuse or misappropriation. The instructions in LinkedIn's "robots.txt" file—a text file used by website owners to communicate with search engine crawlers and other web robots—prohibit access to LinkedIn servers via automated bots, except that certain entities, like the Google search engine, have express permission from LinkedIn for bot access. LinkedIn also employs several technological systems to detect suspicious activity and restrict automated scraping. For example, LinkedIn's Quicksand system detects non-human activity indicative of scraping; its Sentinel system throttles (slows or limits) or even blocks activity from suspicious IP addresses; and its Org Block system generates a list of known "bad" IP addresses serving as large-scale scrapers. In total, LinkedIn blocks approximately 95 million automated attempts to scrape data every day, and has restricted over 11 million accounts suspected of violating its User Agreement,[5] including through scraping.

HiQ is a data analytics company founded in 2012. Using automated bots, it scrapes information that LinkedIn users have included on public LinkedIn profiles, including name, job title, work history, and skills. It then uses that informa-

---

5 Section 8.2 of the LinkedIn User Agreement to which hiQ agreed states that users agree not to "[s]crape or copy profiles and information of others through any means (including crawlers, browser plugins and add-ons, and any other technology or manual work)," "[c]opy or use the information, content or data on LinkedIn in connection with a competitive service (as determined by LinkedIn)," "[u]se manual or automated software, devices, scripts robots, other means or processes to access, 'scrape,' 'crawl' or 'spider' the Services or any related data or information," or "[u]se bots or other automated methods to access the Services." HiQ is no longer bound by the User Agreement, as LinkedIn has terminated hiQ's user status.

tion, along with a proprietary predictive algorithm, to yield "people analytics," which it sells to business clients.

HiQ offers two such analytics. The first, Keeper, purports to identify employees at the greatest risk of being recruited away. According to hiQ, the product enables employers to offer career development opportunities, retention bonuses, or other perks to retain valuable employees. The second, Skill Mapper, summarizes employees' skills in the aggregate. Among other things, the tool is supposed to help employers identify skill gaps in their workforces so that they can offer internal training in those areas, promoting internal mobility and reducing the expense of external recruitment. ...

In May 2017, LinkedIn sent hiQ a cease-and-desist letter, asserting that hiQ was in violation of LinkedIn's User Agreement and demanding that hiQ stop accessing and copying data from LinkedIn's server. ... The letter further stated that LinkedIn had "implemented technical measures to prevent hiQ from accessing, and assisting others to access, LinkedIn's site, through systems that detect, monitor, and block scraping activity."

HiQ's response was to demand that LinkedIn recognize hiQ's right to access LinkedIn's public pages and to threaten to seek an injunction if LinkedIn refused. A week later, hiQ filed suit, seeking injunctive relief ...

The district court granted hiQ's motion. It ordered LinkedIn to withdraw its cease-and-desist letter, to remove any existing technical barriers to hiQ's access to public profiles, and to refrain from putting in place any legal or technical measures with the effect of blocking hiQ's access to public profiles. ...

II. ...

A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest. [The court held that hiQ had established irreparable harm and that balanced of equities tipped in its favor because the "survival of its business is threatened absent a preliminary injunction."]

C. Likelihood of Success ...

2. Computer Fraud and Abuse Act (CFAA) ...

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. ...

HiQ's position is that *Nosal II* is consistent with the conclusion that where access is open to the general public, the CFAA "without authorization" concept is inapplicable. At the very least, we conclude, hiQ has raised a serious question as to this issue.

First, the wording of the statute, forbidding "access[] ... without authorization," 18 U.S.C. § 1030(a)(2), suggests a baseline in which access is not generally available and so permission is ordinarily required. "Authorization" is an affirmative notion, indicating that access is restricted to those specially recognized or admitted. *See, e.g.*, Black's Law Dictionary (10th ed. 2014) (defining "authorization" as "[o]fficial permission to do something; sanction or warrant"). Where the default is free access without authorization, in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of "authorization." *Cf. Blankenhorn v. City of Orange*, 485 F.3d 463, 472 (9th Cir. 2007) (characterizing the exclusion of the plaintiff in particular from a shopping mall as "bann[ing]").

Second, even if this interpretation is debatable, the legislative history of the statute confirms our understanding. …

The 1984 House Report on the CFAA explicitly analogized the conduct prohibited by section 1030 to forced entry: "It is noteworthy that section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' ....' " H.R. Rep. No. 98-894, at 20 (1984). …

We therefore look to whether the conduct at issue is analogous to "breaking and entering." Significantly, the version of the CFAA initially enacted in 1984 was limited to a narrow range of computers—namely, those containing national security information or financial data and those operated by or on behalf of the government. None of the computers to which the CFAA initially applied were accessible to the general public; affirmative authorization of some kind was presumptively required.

When section 1030(a)(2)(c) was added in 1996 to extend the prohibition on unauthorized access to any "protected computer," the Senate Judiciary Committee explained that the amendment was designed to "to increase protection for the privacy and confidentiality of computer information." S. Rep. No. 104-357, at 7. The legislative history of section 1030 thus makes clear that the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort. As one prominent commentator has put it, "an authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web." Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1161 (2016). …

We therefore conclude that hiQ has raised a serious question as to whether the reference to access "without authorization" limits the scope of the statutory coverage to computer information for which authorization or access permission, such as password authentication, is generally required. Put differently, the CFAA contemplates the existence of three kinds of computer information: (1) information for which access is open to the general public and permission is not required, (2) information for which authorization is required and has been given, and (3) information for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed). Public LinkedIn profiles, available to anyone with an Internet connection, fall into the first category. With regard to such information, the "breaking and entering" analogue invoked so frequently during congressional consideration has no application, and the concept of "without authorization" is inapt.

Neither of the cases LinkedIn principally relies upon is to the contrary. LinkedIn first cites *Nosal II*. As we have already stated, *Nosal II* held that a former employee who used current employees' login credentials to access company computers and collect confidential information had acted "'without authorization' in violation of the CFAA." The computer information the defendant accessed in *Nosal II* was thus plainly one which no one could access without authorization.

So too with regard to the system at issue in *Power Ventures*, 844 F.3d 1058 (9th Cir. 2016), the other precedent upon which LinkedIn relies. In that case, Facebook sued Power Ventures, a social networking website that aggregated social networking information from multiple platforms, for accessing Facebook users' data and using that data to send mass messages as part of a promotional campaign. After Facebook sent a cease-and-desist letter, Power Ventures continued to circumvent

IP barriers and gain access to password-protected Facebook member profiles. We held that after receiving an individualized cease-and-desist letter, Power Ventures had accessed Facebook computers "without authorization" and was therefore liable under the CFAA. But we specifically recognized that "Facebook has tried to limit and control access to its website" as to the purposes for which Power Ventures sought to use it. Indeed, Facebook requires its users to register with a unique username and password, and Power Ventures required that Facebook users provide their Facebook username and password to access their Facebook data on Power Ventures' platform. While Power Ventures was gathering user data that was protected by Facebook's username and password authentication system, the data hiQ was scraping was available to anyone with a web browser.

In sum, *Nosal II* and *Power Ventures* control situations in which authorization generally is required and has either never been given or has been revoked. As *Power Ventures* indicated, the two cases do not control the situation present here, in which information is presumptively open to all comers. ...

For all these reasons, it appears that the CFAA's prohibition on accessing a computer "without authorization" is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer. It is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA. The data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using such an authorization system. ...

We note 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 claims may still be available.[15] And other causes of action, such as copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract,

---

15 LinkedIn's cease-and-desist letter also asserted a state common law claim of trespass to chattels. Although we do not decide the question, it may be that web scraping exceeding the scope of the website owner's consent gives rise to a common law tort claim for trespass to chattels, at least when it causes demonstrable harm. *Compare eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) (finding that eBay had established a likelihood of success on its trespass claim against the auction-aggregating site Bidder's Edge because, although eBay's "site is publicly accessible," "eBay's servers are private property, conditional access to which eBay grants the public," and Bidder's Edge had exceeded the scope of any consent, even if it did not cause physical harm); *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 437–38 (2d Cir. 2004) (holding that a company that scraped a competitor's website to obtain data for marketing purposes likely committed trespass to chattels, because scraping could—although it did not yet—cause physical harm to the plaintiff's computer servers); *Sw. Airlines Co. v. FareChase, Inc.*, 318 F. Supp. 2d 435, 442 (N.D. Tex. 2004) (holding that the use of a scraper to glean flight information was unauthorized as it interfered with Southwest's use and possession of its site, even if the scraping did not cause physical harm or deprivation), *with Ticketmaster Corp. v. Tickets.Com, Inc.*, No. 2:99-cv-07654-HLH-VBK, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003) (holding that the use of a web crawler to gather information from a public website, without more, is insufficient to fulfill the harm requirement of a trespass action); *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1364, 1 Cal. Rptr. 3d 32, 71 P.3d 296 (2003) (holding that "trespass to chattels is not actionable if it does not involve actual or threatened injury" to property and the defendant's actions did not damage or interfere with the operation of the computer systems at issue).

or breach of privacy, may also lie. *See, e.g.*, *Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 561 (S.D.N.Y. 2013) (holding that a software company's conduct in scraping and aggregating copyrighted news articles was not protected by fair use).

D. Public Interest ...

[E]ach side asserts that its own position would benefit the public interest by maximizing the free flow of information on the Internet. HiQ points out that data scraping is a common method of gathering information, used by search engines, academic researchers, and many others. According to hiQ, letting established entities that already have accumulated large user data sets decide who can scrape that data from otherwise public websites gives those entities outsized control over how such data may be put to use.

For its part, LinkedIn argues that the preliminary injunction is against the public interest because it will invite malicious actors to access LinkedIn's computers and attack its servers. As a result, the argument goes, LinkedIn and other companies with public websites will be forced to choose between leaving their servers open to such attacks or protecting their websites with passwords, thereby cutting them off from public view.

Although there are significant public interests on both sides, the district court properly determined that, on balance, the public interest favors hiQ's position. We agree with the district court that giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest.

Internet companies and the public do have a substantial interest in thwarting denial-of-service attacks and blocking abusive users, identity thieves, and other ill-intentioned actors. But we do not view the district court's injunction as opening the door to such malicious activity. The district court made clear that the injunction does not preclude LinkedIn from continuing to engage in "technological self-help" against bad actors—for example, by employing "anti-bot measures to prevent, *e.g.*, harmful intrusions or attacks on its server." Although an injunction preventing a company from securing even the public parts of its website from malicious actors would raise serious concerns, such concerns are not present here.

Conclusion

We AFFIRM the district court's determination that hiQ has established the elements required for a preliminary injunction and remand for further proceedings.

QUESTIONS

1. **Ask an Expert**: What would Orin Kerr say about this opinion?
2. **Public and Private**: Is *hiQ*'s distinction between public and private portions of websites convincing? Does this mean that Facebook can stop automated scraping of private user profiles but not automated scraping of public Pages?
3. **Too Legit to Quit**: In another portion of the opinion, the court rejected LinkedIn's argument that it had a "legitimate business purpose" for blocking hiQ. LinkedIn argued that it needed to protect user privacy, protect its investment in building the LinkedIn platform, and enforce its user agreement. How persuasive are these purposes? How about LinkedIn's business goal of

launching its own analytics service competing with hiQ's? Is that legitimate competition, or the very opposite?

4. **Self-Help**: LinkedIn cannot use the CFAA to stop hiQ from scraping its site. Does it follow that LinkedIn cannot even use technical measures to block hiQ?
5. **Automation:** Could LinkedIn ban *all* automated access to its website? Impose rate limits on how many profiles a scraper can access per hour? Allow scraping but require all scrapers to register and identify themselves with each request?