Top of Document

Memorandum
From: Alex Cohen
To: Professor Evelyn Douek
In Re: State Doxxing Laws and Relevant Cases

Executive Summary

The following memorandum summarizes both active and proposed laws in all fifty states (and the District of Columbia) that pertain to either doxxing or similar information-disclosure based offenses. While each state's laws are unique and emphasize different factors, they fall broadly into five major categories:

1. State laws that criminalize or provide civil actions in response to "doxxing" (or "doxing") by name: Alabama, Arkansas, Illinois, Washington

2. State laws that criminalize or provide civil actions in response to an offense that is not called "doxxing" (or "doxing") yet still targets unconsented disclosure private and personally identifying information: Arizona, California, Kentucky, Nevada, Oregon, Texas, Utah, Virginia

3. State laws that criminalize "doxxing," either in name or in spirit (i.e., targeting unconsented information disclosures) only for *certain professions or population subgroups*: Colorado, Minnesota, Oklahoma, West Virginia

4. States that currently have no doxxing laws on their books but that are in the process of adopting laws that target doxxing by name or implication: Florida, Georgia, Massachusetts, New York

5. States/territories that currently have no explicit or implicit doxxing laws on their books but that, if a cause of action for doxxing were brought, might try to reach doxxing conduct under laws for stalking, harassment, cyberstalking, or telecommunications harassment: Connecticut, Delaware, D.C., Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, South Carolina, South Dakota, Vermont, Wisconsin, Wyoming

Note that categories 4 and 5 are not mutually exclusive.

Some brief other points to note: among laws that do not target doxxing specifically or by implication, there are more often than not key limitations that would likely keep the laws from actually targeting doxxing behavior. Two of the most important limits on these laws are *course of conduct* requirements and *mens rea* requirements. First, in order to avoid issues related to free speech, many state laws on harassment/cyberstalking require that two or more acts take place that evidence a unity of purpose across *conduct*, such that it may be proscribed. Second, along similar lines, many states require both a subjective mental state of purpose or knowledge as well

Top of Document

as an objective test for whether an individual would feel harassed, intimidated, or threatened by a given message or act. This is in line with jurisprudence from the Supreme Court like *Counterman v. Colorado*, 600 U.S. ___ (2023).

Below, each state's doxxing laws or closest corollaries are provided, with a brief summary, analysis, and any relevant text provided alongside them. If there are any important cases from a given state's courts either limiting or interpreting the relevant laws on First Amendment challenges, these have also been included with short summaries.

Top of Document

Table of Contents

Executive Summary **1**
1. Alabama **4**
2. Alaska **7**
3. Arizona **8**
4. Arkansas **11**
5. California **13**
6. Colorado **15**
7. Connecticut **17**
8. Delaware **21**
9. District of Columbia **23**
10. Florida **26**
11. Georgia **29**
12. Hawaii **32**
13. Idaho **33**
14. Illinois **34**
15. Indiana **36**
16. Iowa **38**
17. Kansas **40**
18. Kentucky **42**
19. Louisiana **45**
20. Maine **47**
21. Maryland **49**
22. Massachusetts **53**
23. Michigan **54**
24. Minnesota **58**
25. Mississippi **60**
26. Missouri **61**
27. Montana **63**
28. Nebraska **64**
29. Nevada **65**
30. New Hampshire **67**
31. New Jersey **68**
32. New Mexico **69**
33. New York **71**
34. North Carolina **72**
35. North Dakota **73**
36. Ohio **74**

Top of Document

37. Oklahoma.....76
38. Oregon.....78
39. Pennsylvania.....81
40. Rhode Island.....82
41. South Carolina.....84
42. South Dakota.....85
43. Tennessee.....86
44. Texas.....87
45. Utah.....89
46. Vermont.....91
47. Virginia.....92
48. Washington.....93
49. West Virginia.....97
50. Wisconsin.....100
51. Wyoming.....101

Top of Document

1. Alabama
    - *Relevant Provision(s)/Decisions:*
        - ALA. CODE § 13A-11-38 (2024)
            1. Summary
                - Alabama recently criminalized doxxing, making it either a misdemeanor or a felony depending on the frequency of the conduct.
                - While all individuals are protected from doxxing that leads to their harassment or physical injury, the law also singles out certain public officials as subject to greater protections from doxxing that interferes with their "governmental function[s]."
                - PII under the law is construed to include home address, photographs or information about children, or any other information that could expose one to threat.
                - The law also has a strong written-in commitment to free speech norms and ideals
            2. Relevant Text:
                - Important Definitions
                    i. "(a)(4) **Personal Identifying Information includes**, but is not limited to, all of the following:
                        - (A) **Home address**.
                        - (B) **Photographs or information of the victim's children**, including the **schools** they attend.
                        - (C) Any **other information that would enable the victim to be harassed**, **threatened, or harmed**."
                - Actus Reus Defined
                    i. "(b) An individual commits the **crime of doxing** if he or she does either of the following:
                        - (1) **Intentionally** electronically **publishes, posts, or provides personal identifying information of another individual**, with the **intent that others will use that information to harass or harm that other individual, and the other individual is actually harassed or harmed.**
                        - (2) **Intentionally** electronically pu**blishes, posts, or provides personal identifying information of a law enforcement officer, firefighter, or public servant**, with the **intent that others will use that information to harass, harm, or impede the duties of that law enforcement officer, firefighter, or public servant, and the law**

Top of Document

enforcement officer, firefighter, or public servant is actually harassed, harmed, or impeded from performing his or her governmental function."

- Penalties:
  i. "(c)(1) A violation of subsection (b) is a **Class A misdemeanor.**
  ii. (c)(2) A **second or subsequent** violation of subsection (b) is a **Class C felony**."
- Limits:
  i. (d) "Nothing in this section shall be construed to limit any of the following:
    - (1) **Political speech protected by the First Amendment of the United States Constitution.**
    - (2) The publication of contact information of public officials by any individual or organization for the **purpose of encouraging citizens to lobby the public official for or against any policy or legislative act.** For purposes of this subdivision, contact information means an **official address, email, or phone number used by the public official for his or her public service."**

Top of Document

2. Alaska
    - *Relevant Provision(s)/Decisions*:
        - ALASKA STAT. ANN. § 11.61.120 (West 2024)
            1. Summary:
                - Alaska does not have a law that prohibits doxxing specifically; rather, doxxing might be reached as part of the state's criminal prohibition of harassment in the second degree. There is only one narrow place where this can apply, however—repeated threats directed at minors.
            2. Relevant Text:
                - Actus Reus Defined
                    i. "(a) A person commits the crime of harassment in the second degree if, with **intent to harass or annoy another person,** that person:
                        - (7) **repeatedly sends or publishes an electronic communication** that **insults, taunts, challenges, or intimidates** a **person under 18 years of age** in a manner that places the person in **reasonable fear of physical injury** . . ."
                - Penalties:
                    i. "(b) Harassment in the second degree is a **class B misdemeanor**."
        - *McKillop v. State*, 857 P.2d 358 (Alaska Ct. App. 1993)
            1. Summary:
                - Construing the second-degree harassment statute, the Alaska Court of Appeals held that the First Amendment was no bar because it was the **conduct** of contact with an intent to harass that was being proscribed, not the speech itself

Top of Document

3. Arizona
    - *Relevant Provision(s)/Decisions*:
        - ARIZ. REV. STAT. ANN. § 13-2916 (2024)
            1. Summary:
                - Arizona does not have a law that specifically names doxxing and bans it as an offense, but its state harassment statute includes a subdivision that bans the publication of personally identifying information with intent to harass or terrify—or with the intent that a third party harass or terrify the victim as a result of the publication.
            2. Relevant Text:
                - Important Definitions
                    i. "[E.]3. "**Harassment**" means a kno**wing and willful course of conduct** that is directed at **a specific person**, that a **reasonable person would consider as seriously alarming, seriously disruptive, seriously tormenting or seriously terrorizing** the person and that se**rves no legitimate purpose**."
                    ii. "[E.]4. **Personal identifying information**:
                        - (a) Means information that **would allow the identified person to be located, contacted or harassed**.
                        - (b) Includes the person's **home address, work address, phone number, email address or other contact information** that would **allow the identified person to be located, contacted or harassed**."
                - Actus Reus Defined
                    i. "A. It is unlawful for a person to **knowingly terrify, intimidate, threaten or harass** a **specific person or persons** by doing any of the following:
                        - 2. **Threatening to inflict physical harm** on any person or to property in **any electronic communication**.
                        - 3. Otherwise disturbing by **repeated anonymous, unwanted or unsolicited electronic communications the peace**, **quiet or right of privacy of the person** at the place where the communications were received.
                        - 4. **Without the person's consent and for the purpose of imminently causing the person unwanted physical contact**, **injury or harassment by a third party,** use an electronic communication device to

Top of Document

electronically distribute, publish, email, hyperlink or make available for downloading the person's personal identifying information, including a **digital image of the person**, and the use **does in fact incite or produce that unwanted physical contact**, injury or harassment. This paragraph also applies to a person **who intends to terrify, intimidate, threaten or harass an immediate family member of the person whose personal identifying information is used."**

- Penalties:
  - i. "D. A person who violates this section is guilty of a **class 1 misdemeanor**."
- Limits
  - i. "C. This section does not apply to:
    - 1. **Constitutionally protected speech or activity or to any other activity authorized by law**.
    - 2. An interactive computer service, as defined in 47 United States Code § 230(f)(2), or to an information service or telecommunications service, as defined in 47 United States Code § 153, for content that is provided by another person."

- *State v. Musser*, 954 P.2d 1053 (Ariz. Ct. App. 1997), *vacated* 977 P.2d 131.
  1. Summary:
     - Precursor to the law was held overbroad and the court would not engage in a limiting construction; vacated and reconsideration denied by the Arizona Supreme Court.
- *State v. Hagen*, 558 P.2d 750, (Ariz. Ct. App. 1976)
  1. Summary:
     - Precursor to the current law held neither vague nor impermissibly overboard under the First Amendment.

Top of Document

4. Arkansas

- *Relevant Provision(s)/Decisions*:
  - ARK. CODE ANN. § 5-27-610 (West 2024)
    1. Summary:
       - Arkansas prohibits doxxing narrowly, only punishing doxxing that occurs on social media platforms (very broadly construed and possibly inclusive of things like iMessage). The law only applies to minors.
       - Further, it separates its penalties into various classes depending on whether monetary or physical injury (including death) occurs once the threat is made.
    2. Relevant Text:
       - Definitions:
         i. "(a)(2) "Doxxes" means to **publish private or identifying information** about a particular person **on social media** with **malicious purpose**; and
         ii. (a)(3) "Social media platform" means a **website or computer application designed to facilitate communication between one (1) or more persons."**
       - Actus Reus Defined:
         i. (b) A person commits the offense of doxxing of a minor on a social media platform if:
            - (1) The person kno**wingly doxxes or transmits, sends, or posts a communication concerning a minor to a social media platform** with the **purpose to frighten, coerce, intimidate, threaten, abuse, or harass the minor;** and
            - (2) The communication **causes** the **minor to be in reasonable fear of physical injury**.
       - Penalties:
         i. "(c)(1) Doxxing of a minor on a social media platform is a:
            - (A) **Class B felony** if:
              - (i) **Death** of the minor occurs due to the offense; or
              - (ii) Monetary loss to the minor due to the offense is **one million dollars ($1,000,000) or more**;
            - (B) **Class C felony** if:
              - (i) **Physical injury** occurs to the minor due to the offense; or
              - (ii) **Monetary loss to the minor** due to the **offense is ten thousand dollars ($10,000) or more but less**

Top of Document

than one million dollars ($1,000,000); or

- (C) **Class D felony if monetary** loss to the minor due to the offense **is five hundred dollars ($500) or more but less than ten thousand dollars** ($10,000).

ii. (2) Otherwise, **doxxing of a minor on a social media platform is a Class A misdemeanor**.

Top of Document

5. California

- *Relevant Provision(s)/Decisions*:
  - CAL. PEN. CODE § 653.2 (West 2024)
    1. Summary:
       - California's anti-doxxing statute is relatively straightforward, with few complications. It is not cabined to first responders or other public employees and seems to target all harassing and intimidating statements made online that would put a reasonable person in fear of imminent harm.
    2. Relevant Text:
       - Definitions:
         i. "(c) For purposes of this section, the following terms apply:
            - (1) "**Harassment**" means a **knowing and willful course of conduct** directed **at a specific person** that a **reasonable person would consider as seriously alarming, seriously annoying, seriously tormenting, or seriously terrorizing** the person and that **serves no legitimate purpose**.
            - (2) "Of a **harassing nature**" means of a **nature that a reasonable person would consider as seriously alarming, seriously annoying, seriously tormenting, or seriously terrorizing of the person and that serves no legitimate purpose.**
       - Actus Reus Defined and Penalties:
         i. "(a) Every person who, with **intent to place another person in reasonable fear for his or her safety, or the safety of the other person's immediate family**, by means of an **electronic communication device, and without consent of the other person,** and for the **purpose of imminently causing that other person unwanted physical contact, injury, or harassment**, by a **third party, electronically distributes, publishes, e-mails, hyperlinks, or makes available for downloading, personal identifying information,** including, but not limited to, a **digital image of another person,** or an **electronic message of a harassing nature about another person**, which would be **likely to incite or produce that unlawful action, is guilty of a misdemeanor** punishable by **up to one year in a county jail, by a fine of not**

Top of Document

more than one thousand dollars ($1,000), or by both that fine and imprisonment."

- CAL. CIV. CODE §1708.89 (AB No. 1979, Ch. 557)
    1. Summary:
        - California recently chaptered a law that provides a private cause of action for doxing.
    2. Definitions:
        - "Doxes" means an act when a person, with intent to place another person in reasonable fear for their safety, or the safety of the other person's immediate family, by means of an electronic communication device, and without consent of the other person, and for the purpose of imminently causing that other person unwanted physical contact, injury, or harassment, by a third party, electronically distributes, publishes, emails, hyperlinks, or makes available for downloading, personal identifying information, including, but not limited to, a digital image of another person, or an electronic message of a harassing nature about another person, which would be likely to incite or produce that unlawful action.
    3. A prevailing plaintiff may recover:
        - (1) Economic and noneconomic damages proximately caused by being doxed, including, but not limited to, damages for physical harm, emotional distress, or property damage.
        - (2) Statutory damages of a sum of not less than one thousand five hundred dollars ($1,500) but not more than thirty thousand dollars ($30,000).
        - (3) Punitive damages.
        - (4) Upon the court holding a properly noticed hearing, reasonable attorney's fees and costs to the prevailing plaintiff.
- *Dziubla v. Piazza*, 59 Cal. App. 5th 140 (Cal. Dist. Ct. App. 2020)
    1. Summary
        - In a suit between a lender and a borrower, posting the lender's private personal information online was not protected by litigation privileges under California's anti-SLAPP statute.
- *People v. Shivers*, 235 Cal. App. 4th Supp. 8 (Cal. App. Dep't Super. Ct. 2015)
    1. Summary
        - Case applying the doxxing law in the context of a harassment action and parsing the statute to not require that the reasonable fear be of a third party's action

Top of Document

6. Colorado

- *Relevant Provision(s)/Decisions*:
  - COLO. REV. STAT. ANN. § 18-9-313 (West 2024)
    1. Summary:
       - The Colorado doxxing law prohibits doxxing only against certain classes of individuals, but it goes a step further than criminalizing the publication of personal information.
       - In addition to the criminal penalties provided for below, the law also in section (2.8) allows individuals who are doxxed within the meaning of the statute to petition state and local government officials to remove the offending information from the internet and stop it from being republished.
    2. Relevant Text:
       - Definitions:
         i. "(1)(n) 'Protected person' means an **educator, a code enforcement officer, a human services worker, a public health worker, a child representative, a health-care worker, a reproductive health-care services worker**, an officer or **agent of the state bureau of animal protection**, an **animal control officer, an office of the respondent parents' counsel staff member or contractor, a judge, a peace officer, a prosecutor, a public defender, or a public safety worker.**
         ii. "(1)(c) "**Exempt party**" means **any party to the record, a settlement service, a title insurance company, a title insurance agency, a mortgage servicer or a mortgage servicer's qualified agent, or an attorney licensed and in good standing in the state of Colorado** to practice law and who is engaged in **a real estate matter.**"
       - Actus Reus Defined:
         i. "(2.7) It is unlawful for a **person to knowingly make available on the internet personal information** about a **protected person** or the **protected person's immediate family** if the **dissemination of personal information poses an imminent and serious threat to the protected person's safety or the safety of the protected person's immediate family *and*** the **person making the information available on the internet knows or reasonably should know of the imminent and serious threat.**"
       - Penalties:

Top of Document

i. "(3) A violation of subsection (2.7) of this section is a **class 1 misdemeanor**."

- Limits:
  i. "(2.8)(c) An **exempt party** may acces**s a record that includes information otherwise subject to redaction pursuant to subsection (2.8)(b) of this section,** and that is maintained by the **county recorder, county assessor, or county treasurer, if the person seeking access to the record provides evidence and an affirmation under penalty of perjury that they are an exempt party**."

- Colo. Rev. Stat. Ann. §18-9-313.5 (West 2024)
  1. Summary:
     - Expands the doxing statute to include election officials and election workers. Has the same actus reus, penalties, and limits as the doxing statute.
  2. Definitions
     - (b) "Election official" means a county clerk and recorder, a municipal clerk, an election judge, a member of a canvassing board, a member of a board of county commissioners, a member or secretary of a board of directors authorized to conduct public elections, a representative of a governing body, or any other person contracting for or engaged in the performance of election duties. "Election official" includes any person who is an election worker,
     - (c) "Election worker" means a county clerk and recorder, a person currently employed by a county to perform election duties, a municipal clerk, a person currently employed by a municipal government to perform election duties, the secretary of state, and a person currently employed by the secretary of state to perform election duties. "Election worker" does not include an election judge or a temporary employee of a county, municipal government, or the secretary of state.

Top of Document

7. Connecticut

- *Relevant Provision(s)/Decisions*:
  - CONN. GEN. STAT. ANN. § 53A-183 (West 2024) and CONN. GEN. STAT. ANN. § 53A-181D (West 2024)
    1. Summary:
       - These two laws, respectively, Connecticut's Harassment and Stalking in the Second Degree statutes, target intimidation or putting into fear another person using electronic communications. They sweep very broadly, however, which has gotten them in trouble with the state courts (although not yet facially invalidated; *see infra*).
    2. Relevant Text:
       - Definitions:
         i. § 53a-181d:
            - "(3) 'Personally identifying information' means:
              - (A) Any **information that can be used to distinguish or trace an individual's identity**, such as **name, prior legal name, alias, mother's maiden name, Social Security number, date or place of birth, address, telephone number or biometric data;**
              - (B) Any information that is **linked or linkable to an individual, such as medical, financial, education, consumer or employment information, data or records;** or
              - (C) Any other sensitive private information that is **linked or linkable to a specific identifiable individual,** such as g**ender identity, sexual orientation or any sexually intimate visual depiction.**"
       - Actus Reus Defined:
         i. § 53a-183:
            - "(a) A person is guilty of harassment in the second degree **when with intent to harass, terrorize or alarm another person,** and fo**r no legitimate purpose,** such person: (1) **Communicates with a person by telegraph or mail, electronically transmitting a facsimile through connection with a telephone network,**

electronic mail or text message or any other electronically sent message, whether by digital media account, messaging program or application, or otherwise by computer, computer service or computer network, as defined in section 53a-250, or any other form of communication, in a manner likely to cause terror, intimidation or alarm; (2) makes a telephone call or **engages in any other form of communication, whether or not a conversation ensues, in a manner likely to cause terror, intimidation or alarm;** or (3) communicates or shares a photograph, video or words or engages in **any other form of communication to a digital, electronic, online or other meeting space, in a manner likely to cause terror, intimidation or alarm.**

ii. § 53a-181d:
- "(b) A person is guilty of stalking in the second degree when:
  - (3) Such person, **for no legitimate purpose and with intent to harass, terrorize or alarm, by means of electronic communication, including, but not limited to, electronic or social media,** discloses a specific person's **personally identifiable information without consent of the person,** knowing, that **under the circumstances, such disclosure would cause a reasonable person to:**
    - (A) Fear for s**uch person's physical safety or the physical safety of a third person**; or
    - (B) **Suffer emotional distress.**"

- Penalty:
  i. § 53a-183: "(d) Harassment in the second degree is a **class C misdemeanor**."
  ii. § 53a-181d: "(3)(d) Stalking in the second degree is a **class A misdemeanor**."

- *State v. Billings*, 287 A.3d 146 (Conn. App. Ct. 2022)

Top of Document

1. Summary
    - In this case, both state statutes were held unconstitutional as applied to the defendant. The situation is unique, but essentially the defendant was engaged in an extramarital affair with a woman ("A"), who eventually ended things with him. Afterwards, he had a conversation on his Facebook page with a third party (where he and A were no longer friends), discussing the implications if he were to leak photos and messages exchanged between him and A. A only became aware of the conversation on the defendant's page when a friend sent them to her, and the conviction below was brought solely on the basis of this conversation. The court held that this was protected speech that the statutes unconstitutionally tread on.

Top of Document

8. Delaware

- *Relevant Provision(s)/Decisions*:
  - DEL. CODE ANN. TIT. 11, § 1311 (West 2024), DEL. CODE ANN. TIT. 11, § 1312 (West 2024)
    1. Summary: Delaware does not have an anti-doxxing law or even a stalking or harassment law that explicitly applies to communications online. The state law criminalizing harassment, § 1311, primarily applies to telephone calls but has one provision that may be broadly worded enough to capture doxxing. The state anti-stalking law, further, requires at least three separate incidents to transpire before the state is willing to treat them as a concerted "course of conduct."
    2. Potential routes to target doxxing:
       - § 1311:
         i. "(a) A person is guilty of harassment when, with **intent to harass, annoy or alarm another person**:
            - (2) Communicates with a person by telephone, telegraph, mail **or any other form of written or electronic communication** in a manner which **the person knows is likely to cause annoyance or alarm** including, but not limited to, intrastate telephone calls initiated by vendors for the purpose of selling goods or services . . ."
       - § 1312 (assuming the three-incident threshold is met):
         i. "(a) A person is guilty of **stalking** when the person **knowingly** engages in a course of conduct directed at a specific person and that conduct **would cause a reasonable person** to:
            - (1) **Fear physical injury** to himself or herself or that of another person; or
            - (2) **Suffer other significant mental anguish or distress** that **may, but does not necessarily, require medical or other professional treatment** or counseling."
         ii. This law also has aggravating factors for when the victim is a minor or elder, where the intimidator is in possession of a deadly weapon, or where actual physical injury results

Top of Document

9. District of Columbia

- *Relevant Provision(s)/Decisions*:
  - D.C. CODE ANN. § 22-3133 (West 2024)
    1. Summary:
       - D.C. does not have a proper anti-doxxing law, but it does have an anti-stalking statute that targets repeated incidents involving an individual's personal identifying information.
         i. This statute was severely limited, however, by the case cited *infra*, limiting the statute's application to low-value speech categories that are exempted from First Amendment protection.
    2. Relevant Text:
       - DEFINITIONS (FROM D.C. CODE ANN. § 22-3132 (WEST 2024)):
         i. "(8) 'To engage in a course of conduct' **means directly or indirectly, or through one or more third persons**, **in person or by any means**, on **2 or more occasions**, to:
            - (C) **Use another individual's personal identifying information**."
         ii. "(6) 'Personal identifying information' shall have the same meaning as provided in § 22-3227.01(3) [i.e., to include name, address, SSN, tax status, credit card number, signature, biometric data, and the like]."
       - Actus Reus Defined:
         i. "(a) It is unlawful for a person to **purposefully** engage in a course of conduct directed at a **specific individual**:
            - (1) With the **intent** to cause that individual to:
              - (A) **Fear for his or her safety or the safety of another person**;
              - (B) **Feel seriously alarmed**, **disturbed, or frightened**; or
              - (C) **Suffer emotional distress**;
            - (2) That the person **knows** would cause that individual reasonably to:
              - (A) **Fear for his or her safety or the safety of another person**;
              - (B) **Feel seriously alarmed**, **disturbed, or frightened**; or
              - (C) **Suffer emotional distress**;

Top of Document

- (3) That the person **should have known would cause a reasonable person in the individual's circumstances to**:
  - (A) **Fear for his or her safety or the safety of another person**;
  - (B) **Feel seriously alarmed**, **disturbed, or frightened**; or
  - (C) **Suffer emotional distress**."

- Penalties:
  - *i.* *See* D.C. CODE ANN. § 22-3134 (West 2024)
    - There is a complicated regime of fines and prison time laid out here, with aggravations based on prior convictions, causing financial injury, or age difference.
- Limits:
  - i. "(b) This section does not apply to **constitutionally protected activity**"

- *Mashaud v. Boone*, 295 A.3d 1139 (D.C. 2024)
  1. Summary
     - In this case, the D.C. Court of Appeals read the limiting section of the statute (Section (b)) to cabin the statute's reach only those narrow categories of speech that are exempt from First Amendment protection (i.e., low-value speech). The D.C. Court of Appeals found that this limiting construction was the only way the law could remain constitutional, and, applying this construction, reversed and remanded the case for dismissal of the plaintiff's petition for Civil Protective Order.
     - In this case, the plaintiff had his affair with the defendant's wife revealed both in his workplace via email and online via blog posts by the aggrieved defendant-husband.

Top of Document

10. Florida

- *Relevant Provision(s)/Decisions*:
  - S.B. 920, 2024 Leg., Reg. Sess. (Fla. 2024)
    1. Summary:
       - This is a proposed law introduced into the Florida Senate that would create an offense known as "Electronic Harassment." Electronic harassment would use the two-act "course of conduct" threshold, require intent to publish an individual's personal information, require intent to harm or harass, and also include a result element that harm or harassment actually befell the victim.
       - One other unique feature of this proposed law is that it would authorize individuals to bring private civil actions against offenders for both damages and injunctive relief
       - The proposed law also has a limiting clause protecting speech cognizable under the First Amendment
       - If passed, the act will take effect July 1, 2024
    2. Update:
       - Died in Judiciary on Mar. 08, 2024.
  - Fla. Stat. Ann. §836.115 (West 2024)
    1. Summary:
       - This is Florida's law on cyberintimidation by publication, which borrows its definitions of harassment from its generic harassment statute. It's unclear how broadly it has been applied.
    2. Actus Reus:
       - "(2) It is unlawful for a person to electronically publish another person's personal identification information with the intent to, or with the intent that a third party will use the information to:
         i. (a) Incite violence or commit a crime against the person; or
         ii. (b) Threaten or harass the person, placing such person in reasonable fear of bodily harm."
    3. Penalty:
       - "A person who violates this subsection commits a misdemeanor of a first degree."
         i. Punishable by imprisonment of up to one year and/or a fine of up to $1000.
  - FLA. STAT. ANN. § 784.048 (West 2024)
    1. Summary and Relevant Decisions:
       - Cyberstalking is the offense Florida currently has on the books that is most likely to be invoked in targeting doxxing, but it has been limited intensely in Florida's courts. For instance, the courts have made clear that the law

does not apply to isolated communications, even intimidating ones. *See* Bell v. Battaglia, 332 So.3d 1094 (Fla. Dist. Ct. App. 2022). The courts have also been stringent in enforcing the law only where a specific person is named or where the communication is directed at a specific person. *See Wright v. Norris*, 320 So.3d 253 (Fla. Dist. Ct. App. 2021). Where communications have been posted on a medium designed to be read by many people, Florida's courts have held that they cannot be considered directed to a specific person for the purpose of the cyberstalking law. *See, e.g.*, *David v. Textor*, 189 So.3d 871 (Fla. Dist. Ct. App. 2016); *Horowitz v. Horowitz*, 160 So.3d 530 (Fla. Dist. Ct. App. 2015).

- Law also has aggravators for stalking a minor and for violating a restraining order, and it also provides for arrest without a warrant if there is probable cause to believe the law is being violated.

2. Relevant Text:
   - Definitions:
     i. "(b) **'Course of conduct'** means a **pattern of conduct composed of a series of acts over a period of time, however short**, which evidences a **continuity of purpose**."
     ii. "(c) '**Credible threat**' means a **verbal or nonverbal threat**, or a combination of the two, including **threats delivered by electronic communication** or **implied by a pattern of conduct**, which places the person w**ho is the target of the threat in reasonable fear for his or her safety or the safety of his or her family members or individuals closely associated with the person, and which is made with the apparent ability to carry out the threat to cause such harm.** It is **not necessary to prove that the person making the threat had the intent to actually carry out the threat**. The **present incarceration of the person making the threat is not a bar to prosecution under this section.**"
     iii. "(d) **'Cyberstalk'** means:
     - 1. To **engage in a course of conduct to communicate, or to cause to be communicated**, **directly or indirectly**, words, images, or language by or **through the use of electronic mail or electronic communication, directed at or pertaining to a specific person** . . . causing **substantial**

Top of Document

emotional distress to that person and **serving no legitimate purpose**."

- Actus Reus Defined and Penalties:
  - i. "(2) A person who **willfully, maliciously, and repeatedly follows, harasses, or cyberstalks another person commits the offense of stalking,** a **misdemeanor of the first degree** . . .
  - ii. (3) A person who **willfully, maliciously, and repeatedly follows, harasses, or cyberstalks another person and makes a credible threat to that person commits the offense of aggravated stalking,** a **felony of the third degree** . . ."
- Limits
  - i. As defined in 1(b), "The term [course of conduct] does **not include constitutionally protected activity such as picketing or other organized protests."**

Top of Document

11. Georgia

- GA. CODE ANN. § 16-5-90 (West 2024)
    1. Summary
        - This is Georgia's misdemeanor stalking statute, but it likely would not do much to reach doxxing because it is limited to applications where an individual:
            i. "places **under surveillance**, or **contacts another person at or about a place or places without the consent** of the other person for the **purpose of harassing and intimidating the other person**."
        - While there are certainly doxxing instances that would reach this language, most would ostensibly not be included

Top of Document

12. Hawaii

- *Relevant Provision(s)/Decisions*:
  - HAW. REV. STAT. ANN. § 711-1106 (West 2024)
    1. Summary:
       - Hawaii does not have a doxxing statute on its books, but the closest thing is probably its Anti-Harassment statute.
       - This provision requires "intent to harass, annoy, or alarm any other person" and might specifically reach doxxing if the offender:
         i. "(b) **Insults, taunts, or challenges another person in a manner likely to provoke an immediate violent response** or that would cause **the other person to reasonably believe that the actor intends to cause bodily injury to the recipient or another or damage to the property of the recipient or another** . . ."
         ii. Or "(f) Makes a communication **using offensively coarse language** that would cause the recipient to **reasonably believe that the actor intends to cause bodily injury to the recipient or another or damage to the property of the recipient or another**."
       - Since this offense is only a "petty misdemeanor, however, and especially because one of the two ways of reaching doxxing has an offensive language requirement, it is pretty unlikely that this regulation will have sufficient teeth to reach doxxing on its own.

Top of Document

13. Idaho

- *Relevant Provision(s)/Decisions*:
  - IDAHO CODE ANN. § 18-6710 (West 2024); IDAHO CODE ANN. § 18-7902 (West 2024); IDAHO CODE ANN. § 18-7906 (West 2024)
    1. Summary:
       - Idaho does not have a doxxing statute on its books, but the closest thing is probably somewhere between these three statutes on communications security, malicious harassment, and second-degree stalking, respectively
       - Each of these, however, has important limitations that probably keep it from targeting doxxing in a significant way:
         i. For example, the communications security statute, which targets threats and disruptions of the peace directed at specific individuals, only covered communications made by telephone
         ii. Similarly, while the malicious harassment statute targets threats made to intimidate others, it is limited to actions that are motivated by the protected classes of "race, color, religion, ancestry, or national origin"
         iii. Finally, while the anti-stalking statute targets knowing and malicious conduct that "(a) alarms, annoys or harasses the victim and is such as would cause a reasonable person substantial emotional distress; or (b) . . . cause[s] a reasonable person to be in fear of death or physical injury, or in fear of the death or physical injury of a family or household member," it is also limited by the requirement that such acts be part of a course of repeated conduct.
            - This statute is also limited to exclude "constitutionally protected activity"
         iv. Generally, these offenses are punished with fines or imprisonment in Idaho

Top of Document

14. Illinois

- *Relevant Provision(s)/Decisions*:
  - 740 ILL. COMP. STAT. ANN. 195/10 (West 2024)
    1. Summary
       - As of January 1, 2024, Illinois has made it a civil offense to engage in doxxing. It is unclear how broadly the law will be applied due to its numerous explicit limitations on mens rea and its result element, but it is worth noting that the Illinois law is relatively unique in its callout of Section 230 and § 1983 as not precluding any application of the law.
       - Another interesting but unrelated point: Illinois also recently made subject to civil penalty the non-consensual dissemination of deep fake or other digitally altered explicit photographs. *See* 740 ILL. COMP. STAT. ANN. 190/10 (West 2024).
    2. Relevant Text
       - Actus Reus Defined
         i. "(a) An individual engages in the act of doxing when that individual **intentionally publishes another person's personally identifiable information without the consent** of the person whose information is published **and**:
            - (1) the information is published **with the intent that it be used to harm or harass the person whose information is published and with knowledge or reckless disregard that the person whose information is published would be reasonably likely to suffer death, bodily injury, or stalking;** and
            - (2) the **publishing of the information**:
              - (i) **causes the person whose information is published to suffer significant economic injury or emotional distress or to fear serious bodily injury** or **death** of the person **or a family or household member of the person; or**
              - (ii) causes the person whose information is published to **suffer a substantial life disruption**; and

         ii. (3) the person who**se information is published is identifiable from the published personally identifiable information itself**."
       - Limits

Top of Document

i. According to the statute, "(c) Nothing in this Act shall be construed in any manner to:
   - (1) conflict with Section 230 of Title II of the Communications Act of 1934 (47 U.S.C. 230);
   - (2) conflict with 42 U.S.C. 1983; or
   - (3) prohibit any activity protected under the Constitution of the United States or the Illinois Constitution."

ii. The statute also specifies that it will not apply to bona fide reporting activities involving the dissemination of personal information in order to report perceived unlawful conduct. The law also affirms, separately, that it does not apply to
   - "activity protected under the United States Constitution or the Illinois Constitution pertaining to speech, press, assembly, protest, and petition, as well as the provision of personally identifiable information to the press."

Top of Document

15. Indiana

- *Relevant Provision(s)/Decisions*:
  - IND. CODE ANN. § 35-45-2-1 (West 2024); IND. CODE ANN. § 35-45-10-1 (West 2024)
    1. Summary:
       - Indiana does not have a doxxing statute on its books, but it is likely to reach doxxing in some form through a combination of statutes—an anti-intimidation statute and an anti-stalking statute.
       - Indiana's laws have few exceptions and may reach doxxing more easily than some other states' statutes, however, particularly in the case of its intimidation statute, which targets:
         i. "(a) A person who **communicates a threat** with the intent:
            - (2) that another person be placed in **fear of retaliation for a prior lawful act** . . .
            - [or] (4) that another person be placed in **fear that the threat will be carried out"**
              - This includes threats that might:
                - "(6) expose the person **threatened to hatred, contempt, disgrace, or ridicule**;
                - [or] (7) **falsely harm the credit or business reputation of a person** . . ."

         ii. It is unclear, however, whether constitutional limits on the true threat category of low-value speech (after *Counterman*) would allow this offense to be charged as it previously was. It seemingly used to be judged by an objective standard only.
       - Like other state stalking laws, Indiana's anti-stalking law is perhaps not the best candidate to target doxxing behavior because it requires both a course of repeated conduct and also exempts constitutionally protected activity and speech explicitly.
       - Indiana also has an anti-harassment statute on its books, but this statute only seems to target statements made electronically that offend because of their obscene (within the meaning of *Miller*) nature.

Top of Document

16. Iowa

- *Relevant Provision(s)/Decisions*:
  - IOWA CODE ANN. § 708.7 (West 2024)
    1. Summary:
       - Iowa has no explicit doxxing law on its books, but it is possible that this conduct might be targeted by the state's anti-harassment law, which provides:
         i. "1. a. A person commits **harassment** when, with **intent to intimidate, annoy, or alarm another person,** the person does any of the following:
            - (1) Communicates **with another** by **telephone, telegraph, writing, or via electronic communication without legitimate purpose** and in a **manner likely to cause the other person annoyance or harm**."
         ii. This law has been interpreted very strongly, even when related First Amendment challenges have been brought—*see, e.g.*, *State v. Evans*, 672 N.W.2d 328 (Iowa 2003), *State v. Button*, 622 N.W.2d 480 (Iowa 2001).
         iii. Three important limitations, however:
            - No case in Iowa has yet brought up the specific question of whether the First Amendment covers doxxing behavior in itself
            - The law on face seems to only punish communications made *with another* that put *the other* in fear; in other words, the law would not target posts made, for example, on social media and not directed at a particular individual
            - The statute says that "[d]isclosures made in the public interest, including but not limited to the reporting of unlawful conduct, disclosures by law enforcement, news reporting, legal proceeding disclosures, or medical treatment disclosures" are also not covered by the statute. It is unclear how much leeway this would provide a doxxer who believes that their acts are in the public interest.

Top of Document

17. Kansas

- *Relevant Provision(s)/Decisions*:
  - KAN. STAT. ANN. § 60-31A02 (West 2024)
    1. Summary:
       - Kansas does not have an anti-doxxing statute on its books, but its anti-stalking statute may reach doxxing conduct, albeit with several familiar carve-outs.
       - The statute reads:
         i. "(d) 'Stalking' means an **intentional harassment** of another person that places the other person in r**easonable fear for that person's safety**.
            - (1) **'Harassment'** means a **knowing and intentional course of conduct directed at a specific person that seriously alarms, annoys, torments or terrorizes the person, and that serves no legitimate purpose**. . . . (2) **'Course of conduct'** means **conduct consisting of two or more separate acts over a period of time, however short, evidencing a continuity of purpose** which would cause a **reasonable person to suffer substantial emotional distress.**"
         ii. The statute also makes clear, however, that "**Constitutionally protected activity** is not included within the meaning of 'course of conduct.'"
       - As with some other state statutes, however, this statute is potentially limited by the exceptions clause covering constitutional activity, as well as the course of conduct limitation. It is unclear whether the "directed at a specific person" requirement means contact with a specific person, or whether it only requires that a specific person be referenced or named in the harassing message
  - SB 372, 2024 Leg., Reg. Sess. (KS 2024)
    1. Summary:
       - Failed proposal establishing civil liability for doxing.
       - Died in Judiciary on Apr. 30, 2024.
    2. Actus Reus/Definitions:
       - " a person shall not engage in the act of doxing. A person engages in the act of doxing by intentionally publishing another person's personally identifiable information without the consent of the person whose information is published and:
         i. (1) The information is published with the intent that it be used to harm or harass the person whose

information is published and with knowledge that, or with reckless disregard as to whether, the person whose information is published would be reasonably likely to suffer death, great bodily harm, bodily harm or stalking;

ii. (2) the publishing of the information causes the person whose information is published to suffer: (A) Death, great bodily harm, bodily harm or stalking; (B) significant economic injury or emotional distress or to fear great bodily harm or death of the person or a family or household member of the person; or (C) a substantial life disruption; and

iii. (3) the person whose information is published is identifiable from the published personally identifiable information itself. (c) It is not a violation of this section for an individ

Top of Document

18. Kentucky

- *Relevant Provision(s)/Decisions*:
  - KY. REV. STAT. ANN. § 525.085 (West 2024)
    1. Summary:
       - Since its enactment in 2021, Kentucky's law takes a relatively aggressive stance towards doxxing, which it calls "dissemination of personally identifying information."
       - The law casts a wide net of potential individuals who can be statutorily looped in as victims of doxxing, and it also contains no precatory language about constitutional limits attendant to free speech. Its only stated limits apply to providers of information services.
    2. Relevant Text:
       - Definitions
         i. "(1) For the purposes of this section:
            - (a) "**Dissemination**" means **electronically publishing, posting, or otherwise disclosing information to a public Internet site or public forum**;
            - (b) "Household member" means a person who **regularly resides in the household** or who **within the six (6) months preceding the conduct of the offense** regularly resided in the household;
            - (c) "**Immediate family member**" means a parent, grandparent, spouse, child, stepchild, father-in-law, mother-in-law, son-in-law, daughter-in-law, sibling, brother-in-law, sister-in-law, or grandchild; and
            - (d) "**Personally identifying information**" means information that **identifies or reasonably can be used to identify an individual**, including but not limited to:
              - 1. Social Security number or other government-issued identifier;
              - 2. Date of birth;
              - 3. Home or physical address;
              - 4. Electronic-mail address or telephone number;
              - 5. Financial account number or credit or debit card number;
              - 6. Biometric, health, or medical data, or insurance information; or
              - 7. School or employment locations."
       - Actus Reus Defined

Top of Document

i. "(2) A person is guilty of disseminating personally identifying information about another person when, **with the intent to intimidate, abuse, threaten, harass, or frighten a person** who resides in the Commonwealth, he or she:
   - (a) **Intentionally disseminates the personally identifying information** of the person or a person's **immediate family member or household member**; and
   - (b) The **dissemination would cause a reasonable person to be in fear of physical injury to himself or herself**, or to his or **her immediate family member or household member**."

ii. Also applies to any electronic communication that is accessible within the state, regardless of origin

- Penalties
  i. "(4) Disseminating personally identifying information is a **Class A misdemeanor**, unless the dissemination results in:
     - (a) **Physical injury** to the victim or to a victim's immediate family member or household member, in which case it is a **Class D felony**;
     - (b) **Serious physical injury** to the victim or to a victim's immediate family member or household member, in which case it is a **Class C felony**; or
     - (c) **Death of the victim** or of a victim's immediate family member or household member, in which case it is a **Class B felony**."
- Limits
  i. "(5) Nothing in this section shall be construed to impose liability on a broadband **Internet access service provider, a telecommunications service provider, an interconnected VoIP provider, or a mobile service provider** as defined in 47 U.S.C. sec. 153, a **commercial mobile service provider** as defined in 47 U.S.C. sec. 332(d), or a **cable operator** as defined in 47 U.S.C. sec. 522, when acting in its capacity as a provider of those services."

Top of Document

19. Louisiana

- *Relevant Provision(s)/Decisions*:
  - LA. STAT. ANN. § 40:3 (2024)
    1. Summary:
       - Louisiana does not have an anti-doxxing statute on its books, but it does have an anti-cyberstalking statute. In all likelihood, however, this law would not target most doxxing behavior because it only targets the following narrowly defined acts:
         i. "(1) Use in electronic mail or electronic communication of **any words or language threatening to inflict bodily harm to any person** or to **such person's child, sibling, spouse, or dependent, or physical injury to the property of any person, or for the purpose of extorting money or other things of value from any person**.
         ii. (2) **Electronically mail or electronically communicate to another repeatedly,** whether or not conversation ensues, **for the purpose of threatening, terrifying, or harassing any person.**
         iii. (3) Electronically mail or electronically communicate to another **and to knowingly make any false statement** concerning death, injury, illness, disfigurement, **indecent conduct, or criminal conduct of the person electronically mailed** or of any **member of the person's family** or household **with the intent to threaten, terrify, or harass**.
         iv. (4) Knowingly permit an electronic communication device under the person's control to be used for the taking of an action in Paragraph (1), (2), or (3) of this Subsection."
       - Thus, this law could only target repeat instances of doxxing—similar to those that target a course of conduct—under Paragraph (2); doxxing that directly threatens bodily harm under Paragraph (1); or doxxing that misleadingly implies falsehoods about an individual's character or conduct under Paragraph (3)

Top of Document

20. Maine

- *Relevant Provision(s)/Decisions*:
  - ME. REV. STAT. ANN. TIT. 17, § 210-A (2023), *amended via* 2024 ME. LEGIS. SERV. CH. 519 (S.P. 878) (L.D. 2085) (West)
    1. Summary:
       - Maine has no doxxing laws on its books, but like other states, it could potentially reach this conduct through other statutes such as its stalking law (as amended to account for the *Counterman* decision on March 6, 2024).
         i. Maine's harassment law is very narrowly framed and only punishes those who have some affirmative measure taken against them to notify them that their harassing act is unlawful (such as a restraining order, or their current incarceration, etc.)
         ii. Similarly, Maine's electronic harassment law is narrowed to the context of sexual or obscene content being communicated to the victim.
         iii. The stalking law, on the other hand, is more specific than the state's relatively general anti-terrorizing statute (also amended by the emergency legislation of March 6th), and, as amended, punishes those who willfully or knowingly engage in "a course of conduct" directed at or concerning a specific person that "would cause a reasonable person:
              - (1) To suffer serious inconvenience or emotional distress;
              - (2) To fear bodily injury or to fear bodily injury to a close relation;
              - (3) To fear death or to fear the death of a close relation;
              - (4) To fear damage or destruction to or tampering with property; or
              - (5) To fear injury to or the death of an animal owned by or in the possession and control of that specific person."
         iv. Importantly, under the statute, a "'Course of conduct' also includes, but is not limited to, threats implied by conduct and **gaining unauthorized access to personal, medical, financial or other identifying or confidential information.**" It also includes, as amended, not just surveillance, harassment, and interference with property, but also making threats and communications with reckless disregard that they could inspire fear in a reasonable person.

Top of Document

- While there is still a two-or-more-act requirement for behavior to constitute a course of conduct under law, this could open the door to easier prosecution of doxxing behavior under the statute

Top of Document

21. Maryland

- *Relevant Provision(s)/Decisions*:
  - MD. CODE ANN., CRIM. LAW § 3-805 (West 2024)
    1. Summary:
       - Maryland has no doxxing laws on its books, but it does have a very broad provision targeting online harassment—or, as it calls it, "misuse of electronic mail."
       - This statute, however, primarily protects minors against online harassment and, while it does so very strongly (indeed, protecting against even single instances of harassment where narrow criteria are met), it primarily requires that *a course of conduct* be followed and also has a broad exclusions clause for "peaceful activity" undertaken as part of spreading a political message. For single acts, it requires that a request to stop has first been issued.
    2. Relevant Text:
       - Actus Reus Defined
         i. "(b)(1) A person may not **maliciously** engage in a **course of conduct**, through the use of electronic communication, **that alarms or seriously annoys another:**
            - (i) with the **intent to harass, alarm, or annoy the other**;
            - (ii) after **receiving a reasonable warning or request to stop by or on behalf of the other**; and
            - (iii) **without a legal purpose**.

         ii. (2) A person may not use an i**nteractive computer service to maliciously engage in a course of conduct that inflicts serious emotional distress on a minor** or places a **minor in reasonable fear of death or serious bodily injury with the intent**:
            - (i) to kill, injure, harass, or cause serious emotional distress to the minor; or
            - (ii) to place the minor in reasonable fear of death or serious bodily injury.

         iii. (3) A person may not maliciously engage in an electronic communication if:
            - (i) the electronic communication is **part of a series of communications** and has the effect of:
              - 1. intimidating or harassing a **minor**; and
              - 2. causing physical injury or serious emotional distress to a **minor**; and

Top of Document

- (ii) the person engaging in the electronic communication **intends to**:
  - 1. **intimidate or harass the minor; and**
  - 2. cause p**hysical injury or serious emotional distress to the minor.**

iv. (4) A person may not maliciously engage in a **single significant act or course of conduct using an electronic communication if:**

- (i) the person's conduct, when **considered in its entirety, has the effect of:**
  - **1. intimidating or harassing a minor; and**
  - **2. causing physical injury or serious emotional distress to a minor;**
- (ii) the person **intends** to:
  - **1. intimidate or harass the minor; and**
  - **2. cause physical injury or serious emotional distress to the minor; and**
- (iii) **in the case of a single significant act, the communication:**
  - **1. is made after receiving a reasonable warning or request to stop;**
  - **2. is sent with a reasonable expectation that the recipient would share the communication with a third party; or**
  - 3. **shocks the conscience**.

v. (5) A person may not maliciously engage in electronic conduct if:

- (i) the act of electronic conduct has the **effect** of:
  - 1. **intimidating or harassing a minor;** and
  - 2. causing **physical injury or serious emotional distress to a minor;** and
- (ii) the person **intends** to:
  - 1. **intimidate or harass the minor;** and
  - 2. cause **physical injury or serious emotional distress to the minor.**

Top of Document

vi. (6) A person may not violate this section with the **intent to induce a minor to commit suicide."**

- Penalties
  - i. "(e)(1) A person who violates subsection (b)(1), (2), (3), (4), or (5) of this section is guilty of a mi**sdemeanor and on conviction is subject to imprisonment not exceeding 3 years or a fine not exceeding $10,000 or both**.
  - ii. (2) A person who violates subsection (b)(6) of this section is guilty of a **misdemeanor and on conviction is subject to imprisonment not exceeding 10 years or a fine not exceeding $10,000 or both."**
- Limits
  - i. The law does not apply to "peaceable activities":
    - "(1) intended to express a **political view or provide information to others**; or
    - (2) conducted for a **lawful purpose**."
  - ii. Also does not apply to licensed information or communications professionals, as well as those authorized by court order to provide this information

Top of Document

22. Massachusetts

- *Relevant Provision(s)/Decisions*:
  - S.B. 971, 2024 LEG., 193D. SESS. (Mass. 2024)
    1. Summary
       - While Massachusetts does not currently have any doxxing laws on its books, it does have several proposed bills in both the state Senate and House (including the bill linked above), currently in committee, that would refine the state's definitions of stalking, harassment, and state information security requirements to prevent doxxing specifically.
       - Update: Bills still in committee as of Oct. 10, 2024.
       - In the absence of one of these bills being passed, the state could also attempt to rely on MASS. GEN. LAWS ANN. CH. 265, § 43 (West 2024) and MASS. GEN. LAWS ANN. CH. 265, § 43A (West 2024), its stalking and criminal harassment statutes, respectively.
         i. They are perhaps of limited application to doxxing behavior, however, since the stalking offense requires not just suffering of emotional distress on the victim's part, but also an explicit "threat" with an intent to place the victim in "imminent" fear of harm.
         ii. The harassment offense does not require this threat element, but it *does*, like the stalking offense, require that the behavior unfold over a course of conduct.

Top of Document

23. Michigan

- *Relevant Provision(s)/Decisions*:
  - MICH. COMP. LAWS ANN. § 750.411s (West 2024)
    1. Summary
       - While Michigan does not currently have any formal doxxing laws on its books (and attempts to introduce them have died in committee), it does have a prohibition on "posting messages through [an] electronic medium without consent."
       - Though the language of this statute plainly reaches doxxing on its face, it also requires several narrow criteria to be met:
         i. Knowledge that the act can produce a harassing *course of conduct* (2+ incidents)
         ii. Objective threat presented
         iii. Subjective intent to harass
         iv. Result element (conduct does cause harassment or terrorization)
       - The law also expressly excises constitutionally protected activity from its ambit, but cases in Michigan have clarified what this means:
         i. *See* *Buchanan v. Crisler*, 922 N.W.2d 886 (Mich. Ct. App. 2018)
            - While the government had a compelling interest in regulating speech integral to the harassment of private persons, the statute could not be applied to speech relating to public figures on matters of public concern
    2. Relevant Text:
       - Definitions
         i. "(8)(i) 'Post a message' means transferring, sending, posting, publishing, **disseminating, or otherwise communicating or attempting to transfer, send, post, publish, disseminate, or otherwise communicate information, whether truthful or untruthful, about the victim."**
       - Actus Reus Defined
         i. "1) A person shall **not post a message through the use of any medium of communication, including the internet or a computer, computer program, computer system, or computer network, or other electronic medium of communication, without the victim's consent,** if ***all*** of the following apply:
            - (a) The person **knows or has reason to know that posting the message could cause 2 or more separate noncontinuous**

Top of Document

acts of unconsented contact with the victim.

- (b) Posting the message is **intended to cause conduct that would make the victim feel terrorized, frightened, intimidated, threatened, harassed, or molested.**
- (c) Conduct arising from posting the message would **cause a reasonable person to suffer emotional distress and to feel terrorized, frightened, intimidated, threatened, harassed, or molested.**
- (d) Conduct **arising from posting the message causes the victim to suffer emotional distress and to feel terrorized, frightened, intimidated, threatened, harassed, or molested."**

- Penalties
  i. "(2) A person who violates subsection (1) is guilty of a crime as follows:
     - (a) Except as provided in subdivision (b), the person is guil**ty of a felony punishable by imprisonment for not more than 2 years or a fine of not more than $5,000.00, or both.**
     - (b) If any of the following apply, the person is guilty of a felony punishable by **imprisonment for not more than 5 years or a fine of not more than $10,000.00, or both:**
       - (i) Posting the message is in **violation of a restraining order** and the person has received **actual notice of that restraining order** or posting the message is in violation of an injunction or preliminary injunction.
       - (ii) Posting the message is in **violation of a condition of probation, a condition of parole, a condition of pretrial release,** or a condition of release on bond pending appeal.
       - (iii) Posting the message results in a credible threat being communicated to the victim, a member of the victim's family, or another individual

Top of Document

living in the same household as the victim.
    - (iv) The person has been **previously convicted of violating this section** or section 145d, 411h, or 411i,1 or section 6 of 1979 PA 53, MCL 752.796, or a substantially similar law of another state, a political subdivision of another state, or of the United States.
    - (v) The victim is **less than 18 years of age** when the violation is committed and the **person committing the violation is 5 or more years older than the victim."**
- Limits
    i. Does not prohibit "constitutionally protected speech or activity"
    ii. Also does not target information providers or communications services that provide personal information
    iii. Must target conduct that occurs in Michigan, an offender who resides in Michigan, or conduct that is directed at a resident or inhabitant of Michigan.

Top of Document

24. Minnesota

- *Relevant Provision(s)/Decisions*:
  - MINN. STAT. ANN. § 609.5151 (West 2024); HF 4326, 2024 Leg., 93d. Sess. (Minn. 2024)
    1. Summary
       - Minnesota has one very narrow doxxing law on its books and one proposed law targeting doxxing in the state house, respectively.
       - The law on the books that targets doxxing only applies at present to police officers, however, and provides:
         i. "(a) It is a **misdemeanor** for a person to **knowingly and without consent make publicly available**, including but not limited to **through the Internet, personal information about a law enforcement official or an official's family or household member**, if:
            - (1) the dissemination poses an **imminent and serious threat to the official's safety or the safety of an official's family or household member**; and
            - (2) the person maki**ng the information publicly available knows or reasonably should know of the imminent and serious threat.**

         ii. (b) A person is guilty of a gro**ss misdemeanor** if the person violates paragraph (a) and a law enforcement official or an official's family or household member **suffers great bodily harm or death as a result of the violation.**

         iii. (c) A person who is convicted of a **second or subsequent violation** of this section is **guilty of a gross misdemeanor."**
       - The proposed law, on the other hand, would extend similar protections against doxxing to judges and judicial officials in the state.
       - At present, the only law that protects the general public against doxxing behavior in Minnesota is MINN. STAT. ANN. § 609.749 (West 2024), which has similar limitations to the stalking/harassment statutes of different states (limited to true threats, multiple acts). One unique feature of the Minnesota statute, however, is that it includes a crime relating to the use of personal information, albeit one not tied to doxxing: the use of personal information, "without consent, to invite, encourage, or solicit a third party to engage in a sexual act with the person."

Top of Document

2. Updates:
    - The proposed anti-doxing law in the House, HF 4326, died in Chamber as of Apr. 2, 2024.
    - Another similar bill in the Senate, SF3481, also died in Committee on May 20, 2024.

Top of Document

25. Mississippi

- *Relevant Provision(s)/Decisions*:
  - MISS. CODE ANN. § 97-45-15 (West 2024)

1. Summary
   - Mississippi does not have an anti-doxxing law on its books, but the closest thing would be the state's prohibitions on cyberstalking
     i. These, however, are likely to be of limited efficacy in targeting doxxing behavior because they require either the use of a true threat in the message sent to a victim, repeated contact for the purpose of harassment, or the dissemination of false statements with the intent to harass
     ii. In the narrow instances where these indicia are present, however, it is possible that certain doxxing behaviors could be proscribed by law.

Top of Document

26. Missouri

- *Relevant Provision(s)/Decisions*:
  - MO. ANN. STAT. § 565.240 (West 2024)
    1. Summary
       - As of August 2023, Missouri has criminalized doxxing via an offense it calls "Unlawful posting of certain information over the internet."
       - It is framed very broadly and can target even a single instance of doxxing conduct, and it is also not restricted to certain classes of individuals or public employees. Rather; it provides for sentencing enhancements both (a) for protected classes of public employees and (b) for certain result elements (serious bodily harm and death)
    2. Relevant text
       - The relevant law provides, in its entirety:
         i. "1. A person commits the offense of unlawful posting of certain information over the internet if he or she **knowingly posts the name, home address, Social Security number, telephone number, or any other personally identifiable information** of **any person** on the internet **intending to cause great bodily harm or death, or threatening to cause great bodily harm or death to such person.**
         ii. 2. The offense of unlawful posting of certain information over the internet is a **class C misdemeanor, unless the person knowingly posts on the internet the name, home address, Social Security number, telephone number, or any other personally identifiable information of any law enforcement officer, corrections officer, parole officer, judge, commissioner, or prosecuting attorney, or of any immediate family member of such law enforcement officer, corrections officer, parole officer, judge, commissioner, or prosecuting attorney**, intending to cause great bodily harm or death, or threatening to cause great bodily harm or death, in which c**ase it is a class E felony**, and if such **intention or threat results in bodily harm or death to such person or immediate family member,** the offense of unlawful posting of certain information over the internet is a c**lass D felony."**

Top of Document

27. Montana

- *Relevant Provision(s)/Decisions*:
  - MONT. CODE ANN. § 45-5-220 (West 2024)
    1. Summary
       - Montana does not have an anti-doxxing law on its books, but the closest thing would be the state's prohibitions on stalking.
         i. These, however, are likely to be of limited efficacy in targeting doxxing behavior because they primarily target behavior of pursuance, surveillance, and the like. The one narrow overlap with doxxing that is covered by the law may be true threats, but this is on a generous reading.
         ii. It is also worth noting that Montana's law on harassment, MONT. CODE ANN. § 45-5-221 (West 2024), as well as Montana's law on Privacy in Communications, MONT. CODE ANN. § 45-8-213 (West 2024), primarily target lewd and obscene behavior, including the dissemination of private images that are sexual in nature. As such, they are not the best candidates to target doxxing.

Top of Document

28. Nebraska

- *Relevant Provision(s)/Decisions*:
  - NEB. REV. STAT. ANN. § 28-311.03 (West 2024)
    1. Summary
       - Nebraska does not have an anti-doxxing law on its books, but a bill that would have created a doxxing offense died in committee in April 2022. As a result, the closest thing to an anti-doxxing law at present in Nebraska is the state's prohibitions on stalking.
       - The law reads exceptionally vaguely, however, reading in its entirety:
         i. "Any person who **willfully harasses another person** or a family or household member of such person with the **intent to injure, terrify, threaten, or intimidate commits the offense of stalking.**"
            - A previous section of the law defines harassment to include only a course of conduct directed at a specific person with the purpose of intimidation and no other legal purpose.
              - These familiar limitations likely make the law a poor candidate for targeting all but the most serious and repeat instances of doxxing

Top of Document

29. Nevada

- *Relevant Provision(s)/Decisions*:
  - NEV. REV. STAT. ANN. § 41.1347 (West 2024)
    1. Summary
       - Since 2021, Nevada has provided a civil cause of action for those who have been doxxed.
    2. Relevant Text:
       - Tort Defined:
         i. The law provides:
            - "[A] person may bring a civil action against another person if:
              - (a) The other person **disseminates any personal identifying information or sensitive information of the person without the consent** of the person, **knowing that the person could be identified by such information:**
                - (1) With the int**ent to aid, assist, encourage, facilitate, further or promote any criminal offense which would be reasonably likely to cause death, bodily injury or stalking;** or
                - (2) With the **intent to cause harm to the person and with knowledge of or reckless disregard for the reasonable likelihood that the dissemination of the information may cause death, bodily injury or stalking;** and
              - (b) **The dissemination of the personal identifying information or sensitive information**:
                - (1) Would c**ause a reasonable person to fear the death, bodily injury or stalking of himself or herself or a close relation**; or
                - (2) **Causes the death, bodily injury or stalking of the**

Top of Document

person whose information was disseminated or a close relation of the person.

- Liability
  - i. Liability is joint and several for the tort, and a party that prevails in a civil action for doxxing can recover damages, attorney's fees, and costs
  - ii. The law also supports the issuance of an injunction or TRO
- Exceptions
  - i. The law, like many other doxxing statutes, exempts information providers and bona fide reporting activities from the ambit of the law
- Special Features
  - i. While the law incorporates a more common definition of personally identifying information, it also singles out other types of "sensitive information" that may not be disseminated, including sexual orientation, transition status, and HIV status.

Top of Document

30. New Hampshire

- *Relevant Provision(s)/Decisions*:
  - N.H. REV. STAT. ANN. § 633:3-a (2024)
    1. Summary
       - New Hampshire currently does not have a law on its books that specifically targets doxxing, even though one was introduced in 2020 (it died in committee). The closest analogue, then, is its law on stalking.
         i. Like other stalking laws, however, this law is cabined in its application to doxxing by the course of conduct (two or more acts) requirement, though this law is more inclusive than some others by including communications as actions that can comprise a course of conduct.
            - For example, *see* *S.D. v. N.B.*, 306 A.3d 211 (N.H. 2023), which, although not a proper doxxing case, does address the stalking law in the context of particularly aggressive and threatening online posts that mentioned the plaintiff by name or depicted her likeness.

Top of Document

31. New Jersey

- *Relevant Provision(s)/Decisions*:
  - N.J. STAT. ANN. § 2C:12-10 (West 2024)
    1. Summary
       - New Jersey currently does not have a law on its books that specifically targets doxxing. The closest analogue, then, is its law on stalking.
         i. Like other stalking laws, however, this law is cabined in its application to doxxing by the course of conduct (repeated conduct) requirement, and the fact that it can only target threatening speech that puts someone in reasonable fear for their safety.
       - New Jersey also has a cyber-harassment law, but it is mostly focused on lewd and obscene communications. *See* N.J. STAT. ANN. § 2C:33-4.1 (West 2024)
  - SB 2785 and AB 3561, 2024 Leg., Reg. Sess.
    1. Summary:
       - The Senate bill, proposed on Feb. 15, 2024, establishes the crime of doxing. It has been referred to the Senate Judiciary Committee.
       - The Assembly bill, proposed Feb. 5, 2024, has the same format.
    2. Actus Reus:
       - "An actor commits the crime of doxxing if, with the purpose to subject another person, or close relation of that person, to unlawful force, violence, stalking, physical restraint, or mental anguish, or to cause a person to reasonably fear for their own safety or that of another person, the actor knowingly discloses personal identifying information of another person without that person's consent via any electronic device or through a social networking site, and the disclosure of personal identifying information:
         i. (1) creates a substantial risk of serious bodily injury or physical harm to the person or a close relation of that person;
         ii. (2) creates a substantial risk that the person or a close relation of that person is subjected to stalking in violation of section 1 of P.L.1992, c.209 (C.2C:12-10); or

Top of Document

iii. (3) inflicts mental anguish upon the person or a close relation of that person and places the person or the close relation in reasonable fear of physical harm."

- Penalties
  - i. "(1) A violation of this section is a crime of the fourth 19 degree.
  - ii. (2) A violation of this section that results in any serious bodily 21 injury, physical harm, or stalking of a person or a close relation to 22 the person is a crime of the third degree."

Top of Document

32. New Mexico

- *Relevant Provision(s)/Decisions*:
  - N.M. STAT. ANN. § 30-3A-2 (West 2024) and N.M. STAT. ANN. § 30-3A-3 (West 2024)
    1. Summary
       - New Mexico does not have a specific anti-doxxing law on its books, but it does have very broadly framed stalking and harassment laws that could reach doxxing.
       - The harassment law provides:
         i. "A. Harassment consists of knowingly pursuing a **pattern of conduct** that is **intended to annoy, seriously alarm or terrorize another person and that serves no lawful purpose.** The conduct must be such that it would cause a **reasonable person to suffer substantial emotional distress.**
         ii. B. Whoever commits harassment is guilty of a **misdemeanor**."
       - The stalking law provides, in relevant part:
         i. "A. Stalking consists of **knowingly pursuing a pattern of conduct, without lawful authority, directed at a specific individual when the person intends that the pattern of conduct would place the individual in reasonable apprehension of death, bodily harm, sexual assault, confinement or restraint of the individual or another individual.**
         ii. B. As used in this section:
         iii. (1) 'lawful authority' means within the scope of lawful employment or constitutionally protected activity; and
         iv. (2) 'pattern of conduct' means **two or more** acts, on more than one occasion, in which the alleged stalker by any action, method, device or means, directly, indirectly or through third parties, follows, monitors, surveils, threatens or communicates to or about a person.
         v. C. Whoever commits stalking is guilty of a **misdemeanor**. Upon a **second or subsequent conviction, the offender is guilty of a fourth degree felony**. . . ."
       - Thus, while subject to the familiar course of conduct limitation, the two laws nonetheless broadly proscribe a subset of doxxing behavior—that behavior that is intended to threaten or place someone in reasonable fear.

Top of Document

33. New York

- *Relevant Provision(s)/Decisions*:
  - S7646, 2021 Leg., Reg. Sess. (N.Y. 2021)
    1. Summary
       - New York currently does not have any laws against doxxing on its books, but an active bill that has been in committee for since 2022 would create the offense.
         i. In the proposed legislation, the crime would be defined as "knowingly make **restricted personal information** about an individual **publicly available with the intent to threaten, intimidate, or incite the commission of a crime of violence against the individual** or have **intent and knowledge** that the restricted personal information will be used to threaten, intimidate, or facilitate the commission of a crime against the individual."
         ii. The law would also include **"name, telephone number, email addresses and physical or mailing addresses,** which the individual has not made readily apparent to the public, or which the individual has not authorized another person or organization to make readily apparent to the public," as forms of restricted information.
    2. At present, however, it seems New York's only statutory offenses that could reach doxxing are its harassment and intimidation offenses. These, however, require the familiar limitations of either a true threat or a course of conduct to be followed.

Top of Document

34. North Carolina

- *Relevant Provision(s)/Decisions*:
  - N.C. GEN. STAT. ANN. § 14-196.3 (West 2024)

1. Summary
   - North Carolina currently does not have a law on its books that specifically targets doxxing. Its closest analogue is its law on cyberstalking.
     i. North Carolina's cyberstalking law is in some ways quite outdated (not explicitly mentioning social media or any internet platform besides e-mail), but in other ways, it may be broad enough to reach doxxing.
     ii. The law, for example, prohibits: "Electronically mail[ing] or electronically communicat[ing] to another **repeatedly**, **whether or not conversation ensues, for the purpose of abusing, annoying, threatening, terrifying, harassing, or embarrassing any person.**"
        - Taken to include social media posts and other internet communication, this may even be more capable of reaching doxxing than some other state laws.

Top of Document

35. North Dakota

- *Relevant Provision(s)/Decisions*:
  - N.D. CENT. CODE ANN. § 12.1-17-07 (West 2024); N.D. CENT. CODE ANN. § 12.1-17-07.1 (West 2024)
    1. Summary
       - North Dakota currently does not have a law on its books that specifically targets doxxing. Its closest analogues are its law on harassment and stalking, respectively.
         i. Like other state laws on harassment and stalking, however, they are of limited utility in targeting doxxing. The state harassment statute requires, in order for an action to commence, a true threat to be made, obscenity to be communicated, actual repeated contact with no conversational purpose, or the spreading of falsehoods.
         ii. The stalking law, for its part, is also limited in its reliance on the course of conduct standard and its requirement that there be no legitimate purpose behind the actions, in addition to the standard requirements of putting someone in reasonable fear for their safety, etc.

Top of Document

36. Ohio

- *Relevant Provision(s)/Decisions*:
  - OHIO REV. CODE ANN. § 2917.21 (West 2024)
    1. Summary
       - Ohio currently does not have a law on its books that specifically targets doxxing. Its closest analogue, however, is a statute proscribing an offense that the state calls "Telecommunications Harassment." Under Ohio law, computers, telephones, and personal digital assistants are capable of telecommunications, so it is likely that modern smartphones would count too.
         i. In its primary prohibitions, the Ohio law provides:
            - "(A) No person shall **knowingly make or cause to be made a telecommunication, or knowingly permit a telecommunication to be made from a telecommunications device under the person's contro**l, to **another**, if the caller does any of the following:
              - (1) Makes the telecommunication with **purpose to harass, intimidate, or abuse any person at the premises to which the telecommunication is made**, whether or not a**ctual communication takes place between the caller and a recipient** . . .
              - (6) Know**ingly makes any comment, request, suggestion, or proposal to the recipient of the telecommunication that is threatening, intimidating, menacing, coercive, or obscene with the intent to abuse, threaten, or harass the recipient** . . .
              - (10) **Knowingly incites another person through a telecommunication or other means to harass or participate in the harassment of a person**"

         ii. While the mens rea requirements keep this statute from punishing the simple publication of information without knowledge or intent to harass, it seems generally more protective than the average

Top of Document

stalking statute, especially given subsection (A)(10).

Top of Document

37. Oklahoma

- *Relevant Provision(s)/Decisions*:
  - OKLA. STAT. ANN. TIT. 21, § 1176 (West 2024)
    1. Summary
       - As of July 2023, Oklahoma has a law that criminally punishes doxxing on its books. This law, however, is limited only to certain classes of individuals—peace officers, election officials, public officers, and crime victims.
    2. Relevant Text
       - Definitions:
         i. "6. **'Personally identifiable information'** means information w**hich can identify an individual including but not limited to name, birth date, place of birth, mother's maiden name, biometric records, Social Security number, official state- or government-issued driver license or identification number, government passport number, employer or taxpayer identification number, or any other information that is linked or linkable to an individual such as medical, educational, financial or employment information**;
         ii. 7. **'Public official'** means **any person elected or appointed to a state office in the executive, legislative, or judicial branch of state government or other political subdivision of the state . . ."**
       - Actus Reus Defined and Penalties:
         i. "A. Whoever, with the i**ntent to threaten, intimidate or harass, or facilitate another to threaten, intimidate or harass**, uses an **electronic communication device** to **knowingly publish, post or otherwise make publicly available personally identifiable information of a peace officer, public official, election official, or crime victim, and as a result places that peace officer, public official, election official, or crime victim** in **reasonable fear of death or serious bodily injury shall, upon conviction, be guilty of a misdemeanor punishable by imprisonment in the county jail for a term not to exceed six (6) months, or by a fine not to exceed One Thousand Dollars ($1,000.00), or by both such fine and imprisonment**. Upon conviction for a **second or**

Top of Document

subsequent violation, the person **shall be punished by imprisonment in the county jail for a term not to exceed one (1) year, or by a fine not to exceed Two Thousand Dollars ($2,000.00), or by both such fine and imprisonment.**

- Limits
  i. Does not apply to broadcast media or media that is not directed at any given person

Top of Document

38. Oregon

- *Relevant Provision(s)/Decisions*:
  - OR. REV. STAT. ANN. § 30.835 (West 2024)
    1. Summary
       - Since June 2021, Oregon has maintained a civil cause of action against doxxing.
       - The law is not limited to certain classes of individual, but it is limited by both a subjective and objective mens rea inquiry like true threats post-*Counterman*.
       - Separately, a recent court case at the Oregon Court of Appeals has highlighted that when the speech in question is on matters of public importance, the requisite showings under the statute prove much harder.
    2. Relevant Text
       - Definitions:
         i. "(d) 'Personal information' means:
            - (A) The plaintiff's **home address, personal electronic mail address, personal phone number or Social Security number**;
            - (B) **Contact information for the plaintiff's employer**;
            - (C) **Contact information for a family member of the plaintiff**;
            - (D) **Photographs of the plaintiff's children;** or
            - (E) **Identification of the school that the plaintiff's children attend**."
         ii. "Harass" and "stalk" are also defined with reference to the harassment and stalking statutes in Oregon, which bear substantial similarity to the statutes of other states.
       - Tort Defined:
         i. (2) A **plaintiff has a cause of action for improper disclosure of private information** if the plaintiff establishes by a **preponderance of the evidence** that:
            - (a) The defendant, w**ith the intent to stalk, harass or injure the plaintiff, knowingly caused personal information to be disclosed**;
            - (b) The defendant **knew or reasonably should have known that the plaintiff did not consent to the disclosure;**
            - (c) The **plaintiff is stalked, harassed or injured by the disclosure**; and

- (d) A **reasonable person would be stalked, harassed or injured by the disclosure.**

- Remedies:
  - i. "(3) A plaintiff who prevails in a claim under this section may recover:
    - (a) **Economic and noneconomic damages** . . .
    - (b) **Punitive** damages;
    - (c) **Injunctive** relief;
    - (d) **Reasonable attorney fees;** and
    - (e) Any other appropriate equitable relief."
- Limits:
  - i. "(4) An action under this section must be commenced **not later than two years** after the conduct that gives rise to a claim for relief occurred."

- HB 5455, 2024 Leg., Res. Sess.
  1. Summary:
     - This proposal represents an attempt to modernize stalking laws, including a provision against doxing. There is no comparable bill currently in the Senate.
  2. Actus Reus:
     - Causing or attempting to cause a third person to harass, humiliate or injure the other person by disclosing the other person's name, image or personal information, as that term is defined in ORS 30.835, without the consent of the other person.
- *DeHart v. Tofte*, 533 P.3d 829 (Or. Ct. App. 2023)
  1. Summary
     - In this recent case under the Oregon doxxing law, when defendant parents posted the employment information of plaintiff elected school board members (in response to a ban on Black Lives Matter paraphernalia in the school), the Oregon Court of Appeals held that the parent's activity was speech on a matter of public concern protected under the state's anti-SLAPP statute. Accordingly, plaintiffs had failed to state a case for improper disclosure of private information.

Top of Document

39. Pennsylvania

- *Relevant Provision(s)/Decisions*:
  - 18 PA. STAT. AND CONS. STAT. § 2709 (West 2024); 18 PA. STAT. AND CONS. STAT. § 2709.1 (West 2024)
    1. Summary
       - Pennsylvania currently does not have a law on its books that specifically targets doxxing. Its closest analogues are its laws on harassment and stalking, respectively.
       - These statutes are similar to those in other states, however, and they are relatively unlikely to reach doxxing because they retain a course of conduct limitation and a mens rea of purpose/intent.
  - Summary:
    1. Summary:
       - There is a law against endangerment of public safety officials that includes electronic publishing of personal information.
    2. Actus Reus/Mens Rea:
       - **"(a) Endangerment of public safety official.**--A person commits the offense of endangering a public safety official if the person intentionally or knowingly communicates, or publishes through an electronic social media service, the restricted personal information of a public safety official or a family or household member of a public safety official with:
         i. **(1)** Reckless disregard that the restricted personal information will be used to threaten, intimidate or facilitate the commission of a crime against the public safety official or a family or household member of the public safety official; or
         ii. **(2)** The intent that the restricted personal information will be used to threaten, intimidate or facilitate the commission of a crime against the public safety official or a family or household member of the public safety official."
    3. Penalties
       - **"(1)** Except as provided under paragraph (2), an offense under subsection (a) shall constitute a misdemeanor of the first degree."
       - **"(2)** An offense under subsection (a) that results in bodily injury to a public safety official or a family or household member of a public safety official shall constitute a felony of the second degree."

Top of Document

40. Rhode Island

- *Relevant Provision(s)/Decisions*:
  - 11 R.I. GEN. LAWS ANN. § 11-52-4.2 (West 2024)
    1. Summary
       - Rhode Island does not have an anti-doxxing statute on its books specifically, but it does have a very broadly construed cyber-harassment and cyberstalking statute.
       - In its entirety, the statute reads:
         i. "(a) Whoever **transmits any communication by computer or other electronic device** to a**ny person or causes any person to be contacted for the sole purpose of harassing that person or his or her family** is guilty of a **misdemeanor**, and **shall be punished by a fine of not more than five hundred dollars ($500), by imprisonment for not more than one year, or both**. For the purpose of this section, 'harassing' means any **knowing and willful course of conduct directed at a specific person** which seriously alarms, annoys, or bothers the person, and which serves no legitimate purpose. **The course of conduct must be of a kind that would cause a reasonable person to suffer substantial emotional distress**, or be in fear of bodily injury. 'Course of conduct' means a **pattern of conduct composed of a series of acts over a period of time**, evidencing a continuity of purpose. **Constitutionally protected activity is not included within the meaning of 'course of conduct.'**
         ii. (b) A **second or subsequent conviction** under subsection (a) of this section shall be deemed a **felony** punishable by **imprisonment for not more than two (2) years, by a fine of not more than six thousand dollars ($6,000), or both."**
       - Practically, however, this statute may have some difficulty reaching a great deal of doxxing behavior, including not just doxxing that occurs in a single instance but also doxxing that is not directed to or at the victim.

Top of Document

41. South Carolina

- *Relevant Provision(s)/Decisions*:
  - S.C. CODE ANN. § 16-3-700 et seq. (2024); S.C. CODE ANN. § 16-17-430 (2024)
    1. Summary
       - South Carolina does not have a law that specifically bans doxxing on its books, but it, like other states, has anti-harassment and anti-stalking laws that can protect individuals who are put in reasonable fear of harm based on a course of conduct.
       - South Carolina also has an unlawful communications statute that punishes making calls or electronic contact with either the intent to put someone in fear or, when done repeatedly, for the purpose of harassing someone or their family.
       - As the law in South Carolina stands, though, it likely will not reach most types of doxxing that occur over a single instance and lack clear corroboration of the intimidator's mental state

Top of Document

42. South Dakota

- *Relevant Provision(s)/Decisions*:
  - S.D. CODIFIED LAWS § 22-19A-1 (2024)

1. Summary
   - South Dakota lacks a specialized doxxing statute, but as with other states, the closest correlate on the state's books is its stalking statute, which prohibits either making a single credible threat against an individual or repeatedly harassing/contacting them, both in person and online.
   - The emphasis on repeat action, however, familiarly limits the reach of the statute to doxxing behavior.

Top of Document

43. Tennessee

- *Relevant Provision(s)/Decisions*:
  - TENN. CODE ANN. § 39-17-308 (West 2024); TENN. CODE ANN. § 39-17-315 (West 2024)
    1. Summary
       - Tennessee does not have a specific doxxing law on its books, but it—like other states, has closely related statutes in its harassment and stalking laws.
       - As in other states, however, these laws are of limited utility in reaching doxxing conduct because they require either true threats to have been expressed or repeated instances of unwanted conduct to have transpired
       - Interestingly, Tennessee's harassment law also includes a provision whereby even the transmission of a threatening image or video can qualify to inculpate someone under statute.
         i. For example, *see* *Purifoy v. Mafa*, 556 S.W.3d 170 (Tenn. Ct. App. 2017) [therapist making repeated posts on own social media account constituted individual acts incident to stalking offense and not protected speech]

Top of Document

44. Texas

- *Relevant Provision(s)/Decisions*:
  - TEX. PENAL CODE ANN. § 42.074 (West 2024)
    1. Summary
       - Since September 2023, Texas has criminalized doxxing, construed narrowly as an offense called "Unlawful Disclosure Of Residence Address Or Telephone Number"—that is, disseminating the telephone number or address of an individual to a public website with the intent to cause them or family members harm.
       - Like some other laws on stalking and even doxxing, the penalties are graded based on how severe of a harm results from the offense.
       - Finally, the Texas law is limited to not apply to government employees who disseminate such information as part of their jobs, and prosecution under the statute is mutually exclusive of prosecution under the state's obstruction and retaliation statute
    2. Relevant Text:
       - The law reads, in its entirety:
         i. "(a) A person commits an offense if the person posts on a **publicly accessible website the residence address or telephone number** of an **individual with the intent to cause harm or a threat of harm to the individual or a member of the individual's family or household**.
         ii. (b) An offense under this section is a **Class B misdemeanor,** except that the offense is a **Class A misdemeanor if the offense results in the bodily injury of:**
             - (1) the **individual whose residence address or telephone number was posted on a publicly accessible website;** or
             - (2) a **member** of the individual's **family** or **household**.
         iii. (c) This section d**oes not apply to a public servant who posted information described by Subsection (a) to a publicly accessible website** in the performance of the public servant's duties as required by or in accordance with state or federal law.
         iv. (d) If conduct that constitutes an offense under this section also constitutes an offense under Section 36.06(a-1) [Obstruction or Retaliation], the actor

Top of Document

may be prosecuted under either section but not both."

Top of Document

45. Utah

- *Relevant Provision(s)/Decisions*:
  - UTAH CODE ANN. § 76-9-201 (West 2024)
    1. Summary and Relevant Text
       - As of May 2023, Utah has narrowly criminalized and provided a civil form of action against doxxing in the form of an offense called "Electronic Communication Harassment"
       - The rather long statute defining the offense incorporates by reference what seem to be anti-stalking or anti-cyber-harassment standards, then separately goes on to describe a more doxxing-like offense:
         i. "(3) A person is guilty of electronic communication harassment if the person:
            - (a) **electronically publishes, posts, or otherwise discloses personal identifying information** of **another individual in a public online site or forum with the intent to abuse, threaten, or disrupt the other individual's electronic communication** and wit**hout the other individual's permission**; or
            - (b) sends a c**ommunication by electronic mail, instant message, or other similar means**, if:
              - (i) the communication **references personal identifying information of another individual;**
              - (ii) the **person sends the communication:**
                - (A) w**ithout the individual's consent**; ***and***
                - (B) with t**he intent to cause a recipient of the communication t**o **reasonably believe that the individual authorized or sent the communication;** ***and***
              - (iii) with the **intent** to:
                - (A) **cause an individual physical, emotional, or economic injury or damage; or**
                - **(B) defraud an individual**."

Top of Document

- The law punishes electronic communication harassment as a Class B misdemeanor and as a Class A misdemeanor with repeat offenses
- Incorporating a different section of law by reference, the Utah law defines personally identifying information as including:
    i. Name; birth date; address; telephone number; driver license number; social security number; place of employment; employee identification numbers or other personal identification numbers; mother's maiden name; electronic identification numbers; electronic signatures; any other numbers or information that can be used to access a person's financial resources or medical information, except for numbers or information that can be prosecuted as financial transaction card offenses; and a photograph or any other realistic likeness

Top of Document

46. Vermont

- *Relevant Provision(s)/Decisions*:
  - VT. STAT. ANN. TIT. 13, § 1027 (West 2024)
    1. Summary
       - Vermont does not have a specific anti-doxxing statute on its books, but the closest corollary it has is one step more specific than the general anti-harassment and anti-stalking statutes found in other states—specifically, a law that criminalizes "disturbing peace by use of telephone or other electronic communications."
       - This law, however, suffers many of the same shortcomings of the joint harassment-stalking regimes of other states—most prominently, for example, it requires that the acts of contact be repeated
         i. On the other hand, it more laxly punishes not just true threats but also an individual who "disturbs, or attempts to disturb, by repeated telephone calls or other electronic communications, whether or not conversation ensues, the peace, quiet, or right of privacy of any person."

Top of Document

47. Virginia

- *Relevant Provision(s)/Decisions*:
  - VA. CODE ANN. § 18.2-186.4 (West 2024)
    1. Summary
       - Since July 2023, Virginia has narrowly criminalized using personally identifiable information for the purpose of harassment. This isn't quite doxxing in its purest form (no per se violation with a showing of lack of consent), but I'd imagine that it definitely could reach a significant amount of doxxing behavior.
    2. Relevant Text:
       - The law provides, in its entirety:
         i. "It shall be unlawful for any person, with the **intent to coerce, intimidate, or harass another person**, to **publish the person's name or photograph along with identifying information** . . . or i**dentification of the person's primary residence address.** Any person who violates this section is guilty of a **Class 1 misdemeanor.**
         ii. Any person who violates this s**ection knowing or having reason to know that person is a law-enforcement officer** . . . or an **active or retired federal or Virginia justice, judge, or magistrate is guilty of a Class 6 felony**. The sentence shall include a **mandatory minimum term of confinement of six months."**
       - Incorporating another section by reference, this provision defines personally identifying information as inclusive of things like PIN, biometric data, passwords, account numbers, SSN, and so on.

Top of Document

48. Washington

- *Relevant Provision(s)/Decisions*:
  - WASH. REV. CODE ANN. § 4.24.792 (West 2024)
    1. Summary
       - Since July 2023, Washington has explicitly banned doxxing and provided for a civil action against those who have disclosed individuals' personal information without consent.
       - Washington has one of the strongest laws against doxxing, and it has served as a model for some other state laws. It also appears to be the only state that both limits punishable activity in the statute to things outside the protections of the Constitution, while *still* offering a construction note that indicates a preference for liberal construction and victim protection.
    2. Relevant Text:
       - Definitions
         i. "(c) 'Doxing' means **unauthorized publication of personal identifying information** with int**ent or knowledge that the information will be used to harm the individual whose information is published, or with reckless disregard for the risk the information will be used to harm the individual whose information is published."**
       - Actus Reus Defined
         i. "(1) No person may publish an individual's **personal identifying information** when:
            - (a) The **publication is made without the express consent of the individual** whose information is published;
            - (b) The publication is made with:
              - (i) **Intent or knowledge that the personal identifying information will be used to harm the individual whose** information is published; or
              - (ii) **reckless disregard for the risk the personal identifying information will be used to harm the individual** whose information is published; ***and***
            - (c) The **publication causes the individual whose information is published to suffer**:
              - **(i) Physical injury;**
              - **(ii) significant economic injury;**
              (iii) mental anguish;

Top of Document

        - **(iv) fear of serious bodily injury or death for themself or a close relation to themself; or**
        - **(v) a substantial life disruption.**"
    - Civil Action
        i. "(5)(a) An individual whose personal identifying information is published in violation of this section **may bring a civil action against:**
            - **(i) The person or persons who published the personal identifying information; and**
            - **(ii) any person who knowingly benefits, financially or by receiving anything of value, from participation in a venture that the person knew or should have known has engaged in an act in violation of this section.**
        ii. (b) A prevailing claimant who brings a civil action pursuant to this section is **entitled to recover any or all of the following remedies upon request:**
            - **(i) Compensatory damages;**
            - **(ii) punitive damages;**
            - **(iii) statutory damages of $5,000 per violation;**
            - **(iv) costs and reasonable attorneys' fees;**
            - **(v) injunctive relief; and**
            - **(vi) any other relief deemed appropriate by the court.**
        iii. (c) When an action is brought under this section, **a court may, on its own motion or upon the motion of any party, issue a temporary restraining order, or a temporary or permanent injunction,** to restrain and prevent the disclosure or continued disclosure of a party's personal identifying information.
        iv. (d) A civil action **may be brought in any county in which an element of any violation of this section occurred,** or in which an **individual resides who is the subject of the personal identifying information published in violation of this section."**
    - Limits
        i. "(7) The legislature does not intend this section to allow, and this section shall not allow, actions to be brought for **constitutionally protected activity**."
        ii. *See also*:

Top of Document

- "(4) Nothing in this section shall be construed in any manner to:
  - (a) Conflict with 47 U.S.C. Sec. 230;
  - (b) Conflict with 42 U.S.C. Sec. 1983; or
  - (c) Prohibit any activity protected under the Constitution of the United States or the Washington state Constitution."

iii. *But see* the following construction note posted by the Washington legislature:

- "Construction—2023 c 381: 'This act shall be **liberally construed** and **applied to promote its underlying purpose to deter doxing, protect persons from doxing, and provide adequate remedies to victims of doxing**.' [2023 c 381 § 2.]"

Top of Document

49. West Virginia

- *Relevant Provision(s)/Decisions*:
  - S.B. 477, 2024 Leg., Reg. Sess. (W. Va. 2024)
    1. Summary
       - This proposed law, which has been sent to the governor after passing both houses on March 6, will take effect in June and criminalizes doxxing of healthcare workers within certain parameters.
       - Update: signed into law on Mar. 27, 2024.
    2. Relevant Text:
       - Personal information is defined as "**home address, home telephone number, personal mobile telephone number, pager number, personal e-mail address, or a personal photograph or video . . .; directions to the home . . .; or photographs or videos of the home or personal vehicle . . .**"
       - The new offense definition in its entirety provides as follows:
         i. "(b) A **person who knowingly, willfully, and intentionally makes the personal information of a health care worker, or a health care worker's immediate family, publicly available on the internet**:
            - (1) With the intent to **threaten, intimidate, or incite the commission of a crime of violence against that person;** or
            - (2) With the inte**nt and knowledge that the personal information will be used to threaten, intimidate, or facilitate the commission of a crime of violence against that person** is guilty of a misdemeanor and, upon conviction thereof, sh**all be fined not more than $500 or confined in jail not more than six months, or both fined and confined.** For a se**cond or subsequent offense, the person is guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than $1,000 or confined in jail for not more than one year, or both fined and confined."**
  - W. VA. CODE ANN. § 5A-8-24 (West 2024)
    1. Summary
       - This law, also known as Daniel's Law, provides a civil cause of action for "judicial officer[s], prosecutor[s],

federal or state public defender[s], federal or state assistant public defender[s], or law-enforcement officer[s], or any other person residing at the [same] home address" that has their personal identifying information made publicly available under circumstances "in which a reasonable person would believe that providing such information would expose another to harassment or risk of harm to life or property."

- The law also has the following liberal construction disclaimer:
  i. "(b) This act shall be liberally construed in order to accomplish its purpose and the public policy of this state, which is to enhance the safety and security of certain public officials in the justice system, including judicial officers, prosecutors, federal and state public defenders, federal and state assistant public defenders, and law-enforcement officers, who serve or have served the citizens of West Virginia, and the immediate family members of these individuals, to foster the ability of these public servants who perform critical roles in the justice system, and to carry out their official duties without fear of personal reprisal from affected individuals related to the performance of their public functions."

2. Relevant Other Text:
   - Remedies for Tort
     i. "(2) The court may award:
        - (A) Actual damages, but not less than $1,000, for each violation of this act;
        - (B) Punitive damages, if applicable, in accordance with §55-7-29 of this code;
        - (C) Reasonable attorney's fees and other litigation costs reasonably incurred; and
        - (D) Any other preliminary or equitable relief as the court deems appropriate."
   - The law also allows the individuals protected by the law to petition for removal of their information from the internet and provides penalties for those who refuse to remove the offending personal information

Top of Document

50. Wisconsin

- *Relevant Provision(s)/Decisions*:
  - WIS. STAT. ANN. § 947.0125 (West 2024); WIS. STAT. ANN. § 947.013 (West 2024)
    1. Summary
       - Wisconsin does not have a law that penalizes doxxing on its books, but it does have statutes on harassment and unlawful computer communication that may capture some doxxing behavior.
       - Like other state cyber-harassment statutes, however, these only punish repeat instances of contact and true threats that put someone in reasonable fear for their safety, so their utility to target doxxing broadly construed is limited.

Top of Document

51. Wyoming

- *Relevant Provision(s)/Decisions*:
  - WYO. STAT. ANN. § 6-2-506 (West 2024)
    1. Summary
       - Wyoming does not have a law that penalizes doxxing on its books, but its statute on stalking is its closest corollary.
       - Like other state stalking statutes, however, this statute only punishes repeat instances of contact and true threats that put someone in reasonable fear for their safety (using the "course of conduct" standard common in many states), so the utility of this law in targeting doxxing broadly construed is limited.