



Data Privacy Detective Podcast – Episode 71: Doxing and Kentucky’s Pioneering Anti-Doxing Statute

Sep 01, 2021

Categories:

[Blogs](#)

[Podcast](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

[Justin S. Fowles](#)

Kentucky is perhaps the first state to adopt a comprehensive anti-doxing statute that creates a civil tort of doxing, as well as providing explicit criminal penalties for defined doxing conduct. It allows Kentucky residents to sue someone for intentionally disseminating their personal identifying information (PII) with an intent to intimidate, abuse, threaten, harass, or frighten a person or immediate family or household member.

In this podcast episode, [Justin Fowles](#), an attorney in Frost Brown Todd LLC’s Louisville, Kentucky office, shares key insights on what the new law contains and could mean for individuals’ and businesses’ online behavior.

Doxing – or is it doxing? This word entered the Merriam-Webster Dictionary in the 21st century. It defines “dox” as a transitive verb – “to publicly identify or publish private information about (someone) especially as a form of punishment or revenge.” [Dox | Definition of Dox by Merriam-Webster](#). Its origin seems to be a short form of “docs” from the cyber world. It seems to have arisen from hacker groups in the 1990’s that disliked another hacker and went after the victim by spreading the hacker’s personal information, which resulted in harassment like sending multiple pizza deliveries to the target’s home, each driver demanding payment for unwanted food.

Today it connotes cyberbullying or troll harassment by posting personal information about a targeted person or organization, urging others to take action intended to shame or expose the target. Doxing has had tragic ends. Doxed individuals have had surprise visits by SWAT teams breaking down doors to targets’ homes, sometimes resulting in law enforcement killing innocent people based on the doxer’s false message that a kidnapping or domestic violence was occurring there. “Swatting” is a new word with a sinister cyber meaning. [Swatting | Definition of Swatting by Merriam-Webster](#). Teenaged girls have committed suicide from

doxing efforts. Death and more commonly emotional stress arise from doxing attacks.

Doxing does not require programming skills. Doxers can compile and circulate published private identifiable information (PII) about an individual or organization's leaders scraped from legitimate sources, then use the PII to punish, publicly shame, harass, take revenge, or coerce the target to do something they don't want to do (such as paying extortion or ransom to stop the attacks or to avoid release of information about them). Doxing promotes vigilante activity by encouraging others of a like mind to take private action against the target. Doxing has no political or cultural affiliation, as doxing is a tool, not a philosophy. It is agnostic as to victims or users.

A federal anti-stalking statute includes the language "interactive computer service or electronic communication service" within it. 18 U.S.C. § 2261A – [18 U.S. Code § 2261A – Stalking | U.S. Code | US Law | LII / Legal Information Institute \(cornell.edu\)](#). If a person uses such services with intent to kill, harass or otherwise target persons in specific ways that puts them in reasonable fear, causes substantial emotional distress, or otherwise causes them to suffer specified harm, a doxer can be criminally prosecuted. A congressional staffer doxed several U.S. Senators during the confirmation hearings of Justice Kavanaugh and received a 4-year prison sentence, based on several federal criminal statutes. But federal prosecutions are rare, and no U.S. statute was designed specifically to combat doxing.

Enter the states. Kentucky's anti-doxing statute creates a civil tort of doxing, as well as providing explicit criminal penalties for defined doxing conduct. [Kentucky's Anti-Doxing Bill Becomes Law | Frost Brown Todd](#). Effective June 29, 2021, the Kentucky statute was passed by a Republican legislature with Democratic support and signed by a Democratic governor. It allows Kentucky residents to sue someone for intentionally disseminating their personal identifying information (PII) with an intent to intimidate, abuse, threaten, harass, or frighten a person or immediate family or household member. The spread of PII must be such that a reasonable person would be in fear of physical injury to the targeted person or an immediate family or household member. Intent is measured by what would cause a reasonable person to be

in fear of physical injury personally or to a family or household member, rather than requiring express proof of the doxer's actual intent.

Sending an email to another person about someone's personal information would not be an offense. But posting PII about a target to a group in ways defined by the statute could trigger both criminal and civil liability. The statute imposes joint and several liability on those who participate in a doxing attack, activity that could include retweeting someone else's tweet, if the other elements of the tort or crime are proven. This is unlike most torts in Kentucky, which generally apportions liability among tortfeasors rather than making each one liable for the entire damage suffered by a victim.

The courts will be challenged to interpret and apply the statute. Free speech and free association defenses will arise, and there will be constitutional challenges to how the statute will be applied in individual cases. Consider a couple examples. An animal-loving person posts to Facebook a call for others to write to the CEO of a company that the person believes is mistreating animals, providing the CEO's name and email address. Others take action not actually intended by the message sender. Can the originator be prosecuted, be held liable for injury and damage the person did not personally intend? Or a citizen posts a message broadly advocating a position on a controversial topic and tells others where and how to communicate to their legislator, or to a judge considering a criminal sentence, and provides the personal email address or other personal information about the individual targeted for influence. Does the First Amendment trump the anti-doxing statute?

Organizations should consider how best to avoid being either a doxing victim or a doxing perpetrator. Organizations could face civil and criminal challenges under Kentucky's statute as to their use of personal information if communicated within the scope of the statute's reach. Businesses and other organizations should review the personal information they hold and how it is shared or communicated, to avoid being charged with a doxing tort or prosecution. Organizations can likewise review defenses to being doxed. The anti-doxing statute could suggest responses and provide recourse to unfair personal attacks on company personnel.

As individuals, we should all manage our privacy, achieving a balance between the use of our personal information to achieve our objectives in a digital age, but also to prevent hacking, malware, and the unacceptable spread and uses of our personal information. We can limit the amount of personal information that is shared with third parties, seeking to minimize its availability to bad actors. Here are steps individuals can take to reduce the risk of doxing (and other intrusions on our privacy):

- Use a password manager.
- Remove information about you that is available online, by sending opt-out notices to companies that have your personal information. There are services that offer to do this for you for a fee, which include sending opt-out notices to data brokers and others that collect and sell personal information culled from public and other sources. But be aware that most states allow businesses to share personal information of their customers with others as a condition of using those businesses' services, at least when clearly stating to each consumer what information they will share without express consent or the ability to opt-out.
- Use a personal email separate from a business or other email for you and your friends. Consider a separate personal email for websites and firms that require you to post an email, and use that address only for those businesses.
- Visit and use privacy settings (such as your smartphone) to limit sharing of your personal data.
- Don't use Google or Facebook sign-ins on other websites. Enter sites through your own login.
- Don't post your phone numbers or personal email addresses unnecessarily. That won't stop robocalls or a flood of unwanted emails, but it may limit the flow.
- Edit and remove contacts not needed or used currently.

Protecting your personal privacy begins with you.

If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.