

CYBERSECURITY AND DATA PRIVACY

WRITTEN BY SHAWN E. TUMA

Attorney Convicted of Online Impersonation for Fake Prostitution Ads for Exes

An attorney was convicted of online impersonation for setting up false advertisements on Bakepage.com (now defunct) for prostitution services for two women with whom he had prior relationships.¹ Online impersonation requires proof of the following elements: (1) use of the names or personas of another person to create webpages on a commercial social networking site or other internet website; “(2) without obtaining their consent; and (3) with the intent to harm, defraud, intimidate, or threaten any person.”² Law enforcement performed a sophisticated investigation using information obtained from the victims, Backpage.com, as well as the defendant’s Facebook, email, IP address, virtual private network, and prepaid credit cards to connect the defendant to the ads.

Does Access to Messages Obtained Using Opposing Party’s Apple ID—Violate Hacking Law?

A computer forensics firm hired by the husband in a divorce proceeding obtained access to the wife’s personal messages from a third-party’s iPad tablet that their daughter had logged into using the wife’s Apple ID password. The wife brought multiple claims against the forensics firm including a claim under Texas’ civil “hacking law,” Harmful Access by Computer.³ The forensics firm moved for summary judgment arguing there was “effective consent” because the wife had consented to her daughter using the Apple ID on the iPad and the trial court agreed. The appellate court found summary judgment was improper as there was no evidence establishing “effective consent” and, in fact, the wife’s unsworn declaration rebutted any allegation to the contrary.⁴

Does Finding Child Porn on Another’s Cellphone Violate Hacking Law?

An off-duty police officer’s discovery of child porn on a lost, non-passcode protected mobile phone while looking through the phone in an attempt to ascertain its owner did not violate Texas’ criminal “hacking law,” Breach of Computer Security.⁵ The officer acted with the intent to facilitate a legitimate law enforcement purpose, such as community caretaking, and therefore his access of the phone was lawful.⁶ Additionally, whatever subjective expectations of privacy the defendant may have had in the phone, his objective expectation of privacy was limited by the officer’s ability to access it for the purposes of determining ownership.

Does Wife Have Apparent Authority to Consent to Search of iPad Revealing Child Porn?

A wife had apparent authority necessary for her consent to a search of her husband’s passcode-protected iPad to support law enforcement’s search warrant application. The husband

had shared the passcode with his wife. The search resulted in finding child porn on the device and conviction of the husband.⁷

Ransomware Attacks Are Illegal, Paying Their Demands Could Be Also

Using ransomware for extortion is illegal in Texas.⁸ In certain cases it may be illegal for victims of ransomware attacks to negotiate with and make an extortion payment to their attackers to regain access to their computer systems. The U.S. Department of Treasury issued an advisory⁹ cautioning that companies (and those that assist them) that negotiate with and make payments to certain prohibited persons may violate the Treasury’s Office of Foreign Assets Control regulations.

NOTES

1. *Dupuy v. State*, 2020 WL 1942410 (Tex. App.—Houston [14th Dist.] 2020, pet. ref’d).
2. *Id.* at *3 (citing Tex. Penal Code § 33.07(a)(1)).
3. Tex. Civ. Prac. & Rem. Code § 143.001(a).
4. *Tolbert v. Taylor*, 2020 WL 1679234, *9 (Tex. App.—Houston [14th Dist.] 2020, no pet.).
5. Tex. Penal Code § 33.02, et seq.
6. *Oseguera-Viena v. State*, 592 S.W.3d 960, 967 (Tex. App.—Houston [1st Dist.], pet. ref’d).
7. *Gonzalez v. State*, 608 S.W.3d 98, 105 (Tex. App.—San Antonio 2020, pet. filed).
8. Tex. Penal Code § 33.023, et seq.
9. Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Dept. of the Treasury (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.



SHAWN E. TUMA

is an attorney widely recognized in data privacy and cybersecurity law, areas in which he has practiced for over two decades. He is co-chair of the Data Privacy and Cybersecurity Practice Group at Spencer Fane and works primarily in the firm’s Collin County office.