The (Il)legalities and Practicalities of Revenge Porn

By Alex Urbelis

If you watch the *The Newsroom*, you may recall the Season 2 horror, when comely business news anchor, Sloan Sabbith, suddenly realizes that salacious photos of her have been posted on a "revenge porn" site, and were trending on social media.[1] Fiction aside, revenge porn, "or sexually explicit media that is publicly shared online without the consent of the pictured individual,"[2] is a real world problem and becoming increasingly common. The law is reacting, but as is often the case with novel, tech-driven wrongs, most legal redress is cumbersome, ill-fitting, and insufficient.

There are, however, novel legal theories to combat revenge porn at the federal level, and criminal statutes—though of questionable efficacy—at the state level. And, as a practical matter, if a person does share intimate photos, there are technical measures to reduce the likelihood they will remain in another's possession or subject to misuse.

Revenge Porn and the Law

At the Federal Level

A particularly heinous instance of revenge porn involving a current law student has found its way into the U.S. District Court for the Central District of California. Filed by attorneys from K&L Gates, appearing pro bono on behalf of a pseudonymous plaintiff, the complaint alleges that the victim's ex-boyfriend posted sexually explicit material to revenge porn websites, then contacted the victim's friends and colleagues to provide direct links to the obscene material.[3]

This unique federal litigation, seeking injunctive relief and damages, relies on copyright law for jurisdiction. The theory is that since the victim created the images, it is she who owns their copyright. The ex-boyfriend, by posting the images without her consent, is violating the Copyright Act of 1976, entitling the victim to injunctive relief.

There is, however, a major hitch to this approach: relying on copyright law requires that the explicit images be registered with the U.S. Copyright Office. This process is not only cumbersome, but unrealistic and painful for the victim. What is more, assuming the injunction is effective as to the ex-boyfriend, no legal relief can prevent further dissemination of the images. A court can grant relief only regarding a single defendant, and cannot enjoin downstream websites from displaying or transferring the offending images, or prevent search engines, such as Google, from displaying disparaging search results that point to these sites.

Another legal tactic, combating revenge porn with Digital Millennium Copyright Act (DMCA) takedown requests, has sometimes had the opposite of the intended effect. Websites have displayed takedown requests with pride to draw more attention (and clicks) to the offending material. The obvious intent behind this brazen disregard is to discourage future DMCA requests, and it is likely that this audacious tactic is effective.

In sum, copyright law may indeed provide a partial remedy for some patient victims willing to jump through the hoops required of the U.S. Copyright Office, but it is hardly a silver bullet.

Criminalizing Revenge Porn

Defining revenge porn as a criminal act is the clearest signal that this conduct will not be tolerated. Only 13 states criminalize revenge porn, and, technically, New York is not one of them.[4] On the international front, Israel was the first to pass a revenge porn statute and the U.K. the latest to tackle the issue.[5] The mere existence of such laws may be a powerful deterrent. But there are practical considerations for successful prosecutions, and the possibility of foreseeable but unintentional consequences on several fronts.

Chief among practicalities, the law must fit the crime. In New York, the first prosecution of revenge porn failed, largely because existing laws

(continued on page 14)

The (Il)legalities and Practicalities of Revenge Porn

(Continued from page 12)

did not reach this sort of conduct.[6] Harassment was not an option because the material was not sent to the victim herself; unlawful surveillance was inapplicable because the images were created consensually; and the display of offensive materials was similarly inconsonant because nudity is not, per se, offensive.

Responding to this and other failed prosecutions, on 1 November 2014, an amended version of New York's unlawful surveillance statute went into effect, criminalizing the recording or broadcast of images of the sexual or private parts of another which are created without consent.[7] Critics have argued that this amendment does not go far enough to protect victims. As a matter of fit, the law is still not a revenge porn statute—it is a re-engineered version of a peeping tom law. As such, the statute does not extend to sexual material created by mutual consent but distributed without the consent of the victim.

Carrie Goldberg, a board member of the Cyber Civil Rights Initiative, who is active in its 'End Revenge Porn' campaign, notes that: "In New York it's criminal to share credit card numbers[8] and pirated music,[9] yet we have no such protections for the far more personal and devastating distribution of private sexual pictures." Legislation[10] introduced by New York Assemblyman Edward Braunstein would change this, and, according to Goldberg, protect victims regardless of the motive of the distributor, "whether for revenge, entertainment, money, 'lulz,' or no reason at all."[11]

Another practical reason prosecutions fail is for a lack of resources. Revenge porn is a fast-moving, cross-border offense that occurs on several different technological platforms: cameras, smart phones, and web servers. Most local law enforcement and prosecutors do not have the financial, technical, or human resources to track and collect transient forensic evidence across several jurisdictions.

Disappearing Evidence and False Flags

A clear-cut case would look like this: a victim is notified of offending material that can be traced back to an image sent to an ex-boyfriend. The mobile device of that ex-boyfriend contains the image distributed without consent, and distribution can be traced to his IP address and his mobile device. Prosecutions, however, are rarely so straightforward.

The first stumbling block is the image itself. If neither the victim nor the ex-boyfriend have a record or copy of the image (perhaps both upgraded their devices or deleted old messages), then only their mobile carrier(s) will have a record of the initial transmission. Acquiring that data is time-consuming and resource-intensive.

But assuming no problem with the above, the next evidentiary hurdle is proof of distribution. Some exes may be so incensed as to throw caution to the wind, but a thoughtful offender would use a new device and public wi-fi for distribution. Technically astute offenders would use a throwaway device and a virtual private network (VPN), to make it seem as if the distribution originated from China or Russia. Acquiring logs and connection data from a foreign VPN provider (if such records are even kept) is both a crapshoot and a herculean task.[12] But in the prosecutorial context, if you combine this type of anti-forensic behavior with the fact that mobile devices are often lost or stolen, and add to that the prevalence of data breaches and malware, you have something that begins to look very much like reasonable doubt.

With evidence difficult to collect and resources scarce, failed prosecutions may have serious unintentional consequences: discouraging victims from coming forward, deterring further prosecutions, and emboldening potential offenders.

Practical Advice for Cautious Couples

The best way to ensure images never make their way to revenge porn sites is obvious: do not create them. If, however, a person chooses to take and share intimate photos, there are technical measures that can decrease the likelihood of the image being retained and misused.

First: do not send intimate pictures through text message, iMessage, Whatsapp, or any other messaging platform that creates a continuous historical record of activity. Doing so makes it easy for a spurned lover to scroll backwards in time and find revealing photos exchanged during better times.

Second: if you do share private photos, use third-party messaging applications such as Wickr, Silent Circle, or Snapchat that "burn" images after a specified period of time. With these apps, it is possible to specify that the message or image remain with the recipient for as little as ten seconds. While this does not prevent screen captures of images, it does prevent a person from retrieving previously sent images. Further, apps such as Wickr and Snapchat make executing the screen capture function on an iPhone a more cumbersome process, reducing the likelihood that an image will be stored. Snapchat, by the far the most popular app for sharing intimate photos, alerts senders when an image has been screen captured.[13]

Third: if sharing is not the goal, do not use an Internet-enabled device to capture private moments. Recall the standalone digital camera, the long-forgotten device used to take pictures and nothing more. Placing several steps between yourself and transmission of a private photo will make it less likely to occur.

Fourth: do not back up intimate photos to a cloud. Many devices, including iPhones, are configured, by default, to keep photos in a cloud's central repository. Weak passwords and angry exes are an awful combination, and the cloud is an all too easy target.

Fifth and finally: Though unsexy, keep a detailed log of images sent and to whom they are sent. If the relationship devolves into a revenge porn fiasco, those contemporaneous records could be critical to a successful prosecution when evidence from other sources is lacking.

* * *

Technology will always outpace legislation. It is, therefore, no surprise that the legal remedies available to victims of revenge porn are inadequate. Federal remedies are slow, burdensome, expensive, and only partially effective. Criminalizing revenge porn is a strong statement, but also an imperfect solution because of the under-inclusive nature of the proscribed conduct and the ease with which evidence can be destroyed and prosecution frustrated.

What is clear, however, is that victims of revenge porn are seriously and irreparably harmed. The elements and mechanics of criminal statutes and the civil remedies available require further consideration and study. Unless and until such a time, the best defense is a good offense. The more we understand the permanence of our digital footprints and the technical measures at our disposal to reduce them, the better able we, as users, are to avoid the problem of revenge porn altogether.

Endnotes

1. Alan Everly, *'The Newsroom' Recap: Sloan's Nude Photos Go Viral; Maggie's Losing It*, L.A. Times, 12 August 2013, http://lat.ms/1DCD0gz.
2. Revenge Porn, Wikipedia, http://bit.ly/1u7p46r.
3. Civil Lawsuit on Revenge Porn, N.Y. Times, http://nyti.ms/1AKnHMA.
4. Revenge Porn: U.S. Laws, Wikipedia, http://bit.ly/1MNupZG.
5. Rick Kelsey, Revenge Porn is Being Made a Specific Criminal Offence, BBC Newsbeat, http://bbc.in/1FB7HjL.
6. *People v. Barber*, 42 Misc. 3d 1225(A) (N.Y. City Crim. Ct. 2014).
7. N.Y. Penal Law § 250.45.
8. N.Y. Penal Law § 165.17.
9. A7811B-2011 (N.Y. 2011); N.Y. Penal Law § 275.00.
10. B. A571, 2015 Assem., Reg. Sess. (N.Y. 2015).
11. New York's proposed revenge porn law establishes as the crime of non-consensual disclosure of sexually explicit images as a class A misdemeanor. The bill is available at http://bit.ly/1GuN3Sy.
12. TorGuard, a prominent VPN provider, advertises that it does not keep logs of activity associated with an IP address. Further, it notes that hundreds of users are using any server at any particular time, making attribution of activity nearly impossible. *See,* Do You Keep Any Log Files, TorGuard, http://bit.ly/1B5UMlv.
13. A cottage industry of third party applications that surreptitiously capture Snapchat images has developed. However, in recent months, Snapchat has implemented more sophisticated alert measures to combat this. Nothing, however, would detect whether a separate device, such as a camera, was used to photograph the screen of the recipient's phone while the image was displayed.

Alex Urbelis is a lawyer and hacker with over 20 years of experience with information security. He has worked for the U.S. Army, the Institute for Security Technology Studies at Dartmouth, the CIA, the U.S. Court of Appeals for the Armed Forces, Steptoe & Johnson, and as information security counsel and CCO of Compagnie Financière Richemont SA (Richemont). Alex holds a BA, summa cum laude, in Philosophy from Stony Brook University, a JD, magna cum laude, from Vermont Law School, and the BCL from New College, University of Oxford.