Berkeley Journal of Entertainment and Sports Law

Volume 7 | Issue 1 Article 5

7-1-2018

Lessons from Hollywood Cybercrimes: Combating Online Predators

Robert Kang

Link to publisher version (DOI)
https://doi.org/10.15779/Z38WH2DF3Q

Lessons from Hollywood Cybercrimes: Combating Online Predators

By Robert Kang•

Everyone has emails and other digital information that they consider to be no one's business except their own. Our emails contain everything from tax returns to intimate photos meant only for someone special. Imagine the horror if a hacker infiltrated an email account belonging to someone you knew and made those emails public. Imagine the horror if it happened to you.

For many people, no imagination is needed because it did happen to them. This type of hacking is a crime and many hackers have been brought to justice. But that doesn't change the horror of being victimized. This article walks

DOI: https://doi.org/10.15779/Z38WH2DF3Q

• Robert Kang is an adjunct professor of technology at Loyola Law School, Los Angeles, where he helped create Southern California's first cybersecurity and data security law concentration. He is also in-house counsel at a Fortune 500 company focusing on cybersecurity, intellectual property and contracts. The views expressed in this article are his own. Follow him on Twitter: @CyberSecEsq or on LinkedIn: www.LinkedIn.com/in/CyberSecEsq. Email: kangr@lls.edu

through some of the nation's most well-known hacks and shares tips for responding to similar attacks. Whether you're a corporate executive protecting company secrets or a college student protecting personal emails, there are many techniques for protecting online information. Learning them through these examples may help protect yourself, your business, and your loved ones from hackers.

Part 1: Protecting Yourself From 2010's "The Man Who Hacked Hollywood" (Password Challenge Questions)

Renee Olstead is an actress and singer. Olstead started acting when she was five years old, and has appeared in shows like "Touched by an Angel" and "The Secret Life of the American Teenager." She works hard and has a bright future. Olstead is also a survivor of sex-based computer hacking.

In 2010, a then-unknown hacker hacked into Olstead's personal email accounts. Her private photos, including nude photos, appeared on the internet, where they spread like wildfire.[1] It was a gross violation of her privacy. Olstead even attempted suicide, though fortunately wasn't successful.[2] She was only 21 at the time.

Olstead shared her story to a court in 2012 as follows: "about two years ago, I received a phone call from [FBI] Agent [Josh] Sadowski informing me that my personal information had been compromised. And basically that it was a matter of time before these images hit the internet . . . I was humiliated."[3]

Olstead wasn't alone. Between November 2010 and October 2011, the FBI tied over 50 victims to Olstead's hacker.[4] The list reflected a "who's who" of Hollywood: Scarlett Johansson, Mila Kunis and Christina Aguilera, among others.[5] The widespread sharing of their intimate photos online created one of the most graphic events in American cyber history.[6] This mysterious assailant

---

1. Olstead's story is available at Appellant's Excerpt of Record (Vol. I) at ER9, ER57-ER60, *United States v. Chaney*, No. 13-50015 (9th Cir. Dec. 18, 2014), ECF 13-3 ("Chaney AER (Vol. 1)"). The portion cited is a transcript of Christopher Chaney's sentencing proceeding, and it transcribes Ms. Olstead's Victim Impact Statement to the Court.

2. *Id.*

3. *Id.* at ER58.

4. Described in the Plea Agreement of Christopher Chaney. The Plea Agreement is available at Appellant's Excerpt of Record (Vol. 2), at ER106, ER117, *United States v. Chaney*, No. 13-50015 (9th Cir. Dec. 18, 2014), ECF 13-4 ("Chaney AER (Vol. 2)").

5. *Id.*

6. Many news articles were written about this incident. One of the most comprehensive was written by a GQ reporter, who interviewed Chaney. David Kushner, *The Man Who Hacked Hollywood*, GQ, April 24, 2012, at 150 "GQ Interview"). An online reprint is available at

became known as "The Man Who Hacked Hollywood."[7]

Spoiler alert: the case ends with Olstead and Johansson learning their hacker's identity, and even delivering some payback. In 2011, the FBI tracked down and arrested Christopher Chaney, a then–35 year old man living in Jacksonville, Florida.[8] One technique used by law enforcement to find hackers involves tracking their Internet Protocol (IP) address. Think of an IP address as the internet version of a calling card which is left behind when one computer talks with another.[9] Chaney had evaded capture using a service called "Hide My IP," which masked his IP address.[10] However, the FBI was watching, and the one time Chaney slipped, the FBI pounced.[11] On February 10, 2011, armed with a warrant, the FBI raided Chaney's home for evidence. Eight months later he was arrested and successfully prosecuted.[12] The trial court sentenced Chaney to ten years, and his sentence was affirmed on February 22, 2016, by the United States Court of Appeals for the Ninth Circuit.[13] Barring the unexpected, Chaney will remain a guest of the penal system for many years.[14]

The sentencing phase of Chaney's prosecution is where Olstead and Johansson came in. Survivors may fear speaking in court, which requires them to share intimate pain in a very public setting. But victim impact statements are invaluable to putting criminals behind bars.[15] Olstead recounted her experiences in court. "I realized that suddenly I wasn't the girl who works full time, is a full-

---

http://www.davidkushner.com/article/the-man-who-hacked-hollywood/.

7. *Id.*

8. Chaney AER (Vol. 2), *supra* note 4, at ER120 (Plea Agreement); FBI Press Release, *Florida Man Arrested in "Operation Hackerazzi" for Targeting Celebrities with Computer Intrusion, Wiretapping, and Identity Theft* (Oct. 12, 2011), *at* https://archives.fbi.gov/archives/losangeles/press-releases/2011/florida-man-arrested-in-operation-hackerazzi-for-targeting-celebrities-with-computer-intrusion-wiretapping-and-identity-theft ("Chaney Arrest Press Release").

9. This is a simplified summary of an IP address. For a layperson explanation, visit Michael Horowitz, *What does your IP address say about you?*, CNET (Sept. 16, 2008), *at* https://www.cnet.com/news/what-does-your-ip-address-say-about-you/.

10. Chaney AER (Vol. 2), *supra* note 4, at ER119 (Plea Agreement).

11. Michael Sohn, Lisa Feldman, Robert Kang, Jennifer McGrath, CLE Presentation at UCLA School of Law, *Cybersecuring Hollywood Part II* (Oct. 13, 2015) ("Cybersecuring Hollywood II").

12. Chaney Arrest Press Release, *supra* note 8.

13. *United States v. Chaney*, 628 Fed. Appx. 492 (9th Cir. Dec. 30, 2015).

14. Give Chaney points for continuing to challenge his sentence: on May 15, 2017, he filed for a writ of *habeus corpus* (essentially a different type of appeal), claiming ineffective assistance of counsel. Motion to Vacate, Set Aside, or Correct Criminal Conviction and Sentence Pursuant to 28 U.S.C. § 2255 by a Person in Federal Custody, *United States v. Chaney*, No. 211-CR-00958-SJO, CV 17-3653 (C.D. Cal May 15, 2017). In the author's opinion, Chaney's chances are slim.

15. This is the author's opinion after speaking with many law enforcement officers. *See also* Chaney AER (Vol. 1), *supra* note 1, at ER15-ER21 (in sentencing Chaney, the judge described the Victim Impact Statements as "[q]uite moving impact statements. . .I think it's helpful for the court to have these victim impact statements so that the Court has an appreciation for the harm that's been caused.").

time student who still manages to make the Dean's List," she told the judge. "Instead, I was [now] the girl who was naked on the internet. And this is something that has followed me . . . it was the scariest moment of my life."[16] Johansson also shared her story in court, via a recorded video statement. "I have been truly humiliated and embarrassed," she said. "I find Christopher Chaney's actions to be perverted and reprehensible. As long as he has access to a computer, Christopher Chaney continues to be a threat to women who believe email communications are personal and confidential."[17]

These statements touched the judge, who referenced them, and other victims' statements, in sentencing Chaney. [18] Chaney's ten-year sentence was nearly twice the length proposed by prosecutors.[19]

How did Chaney hack into his victims' online accounts? Was he a computer genius? A seasoned hacker who played electronic hide-and-seek with the NSA in his spare time?

The answer might surprise you.

Chaney was not a professional hacker.[20] But he was a social engineer of sorts, and clever enough to figure out how people answer the "challenge questions" used by many online service providers to help users reset a lost or forgotten password.[21] We've all seen them: "What is your pet's name?" or "What is the make of your first car?" Most of us don't think twice about answering those questions honestly. Neither did many of Chaney's victims.[22] That inclination to honesty gave Chaney his chance.

Like a detective, Chaney studied his targets: famous women. He read magazines and news articles about them; he subscribed to online sources and databases like IMDB that compiled celebrity dossiers.[23] This careful research enabled Chaney to figure out the answers to many of the celebrity's email password reset challenge questions. For example, in one instance, Chaney

---

16. Chaney AER (Vol. 1), *supra* note 1, at ER 58 – ER 60 (transcript of Victim Impact Statement).

17. *Id.* at ER89-ER90.

18. *Id.* at ER1-ER8 (Judgment and Probation/Commitment Order); ER15-ER21 (Judge considers victims' statements in calculating Chaney's sentence).

19. *Compare* Chaney AER (Vol. 2), *supra* note 4, at ER227-53 (Government's Position re. Sentencing of Defendant Christopher Chaney; Exhibit)(proposing a 71-month sentence); *with* Chaney, 628 Fed. Appx. 492, at *passim* (affirming the District Court's imposition of a 120 month sentence).

20. GQ Article, *supra* note 6, at 250.

21. *Id*. *See also* Chaney AER (Vol. 2), *supra* note 4, at ER117-ER118 (Plea Agreement describing Chaney's actions).

22. *See* sources cited, *supra* note 21.

23. *Id.*

successfully hacked into one celebrity's account using the name of her pet.[24] After gaining access to the victim's account, Chaney set it to automatically forward the victim's emails to other accounts controlled by Chaney. When the victim found herself locked out of an account, she assumed it was an electronic glitch and simply reset it. But, like many of us, she didn't think to check whether the account had been altered to forward emails automatically to someone else's email account.[25]

Chaney's sleuthing opened him up to a treasure trove of personal information. He learned about Scarlett Johansson's separation from Ryan Reynolds before the news became public, for example.[26] Before being arrested, Chaney also harvested intimate celebrity photos, many of which he shared with others.[27] The rest is internet history.

Part 1 Tips:

- Be strategic when providing answers to password reset challenge questions. Don't use your actual mother's maiden name, for example, but rather a word that only you would know. Changing this habit goes a long way to protecting your online information.

- Be suspicious if you can't open an email account. If your password doesn't work, don't assume it's a glitch. Instead, treat it as a potential hack. Check that your account settings haven't been tampered to forward emails automatically to a different email account.

- Want to learn more about challenge questions? There are many articles on the subject: Click HERE – Security Questions Don't Protect You: Here's Why.[28]

Part 2: Protecting Yourself from 2014's "Celebgate" Hackers (Phishing Emails)

Crime never stops. Two years after Chaney's capture came "Celebgate" (aka "the Fappening") – the name of a hacking spree that, again, resulted in the viral posting of intimate photos belonging to famous celebrities like Jennifer

---

24. *Id.*
25. Chaney AER (Vol. 2), *supra* note 4, at ER118 (Plea Agreement describing Chaney's actions).
26. GQ Interview, *supra* note 6, at 253.
27. *Id. See also* Chaney AER (Vol. 2), *supra* note 4, at ER119 (Plea Agreement).
28. Jordan Holtz, *Security Questions Don't Protect You: Here's Why*, IAPP Privacy Advisor (April 22, 2014), https://iapp.org/news/a/security-questions-dont-protect-you-heres-why/.

Lawrence and Kate Upton.[29]

But while the attacks continued, so did the government's commitment to capturing the guilty. On March 15, 2016, the FBI and the United States Attorney's Office announced that a then-36 year old Pennsylvania man, Ryan Collins, signed a plea agreement, requiring him to plead guilty to violating the Computer Fraud and Abuse Act, a federal law which prohibits unauthorized access to a protected computer system laws.[30] He is one of several criminals caught in connection with Celebgate, all of whom used similar techniques to gain unlawful access to their victims' personal information.[31]

In order to gain access to his victims' accounts, Collins, and others like him, engaged in "phishing" – a hacking technique that involves creating fake email accounts that look trustworthy.[32] For example, Collins created email accounts with names like "secure.helpdesk0019@gmail.com."[33] Using these fake accounts, Collins sent emails to celebrities, asking them (or asking the people managing those accounts) for account and password information. If he was successful, Collins downloaded the contents of a victim's email or cloud storage account.[34]

Collins was sentenced on October 26, 2016, in a federal courthouse located in Harrisburg, Pennsylvania, to 18 months in prison.[35] But justice doesn't sleep. Since then, federal agents have successfully nabbed three more hackers associated with Celebgate: Edward Majerczyk of Chicago, Illinois; Emilio

---

29. There were many articles written about Celebgate. Here's one: Daniel Stoller, *And the Oscar Goes to False Hollywood Cybersecurity Horror Story*, Bloomberg BNA - Privacy and Data Security Blog (Feb. 24, 2017), https://www.bna.com/oscar-goes-hollywood-b57982084382/.

30. United States Department of Justice Press Release, *Pennsylvania Man Charged With Hacking Apple and Google E-Mail Accounts Belonging to More Than 100 People, Mostly Celebrities* (March 15, 2016), *at* https://www.justice.gov/usao-cdca/pr/pennsylvania-man-charged-hacking-apple-and-google-e-mail-accounts-belonging-more-100 ("Collins Press Release")

31. Gene Maddaus, *Fourth Celebgate Suspect Pleads Guilty to Hacking Charge*, Variety (Jan. 11, 2018), *at* http://variety.com/2018/biz/news/george-garofano-celebate-plea-1202662591/. For more detail, *see* (1) Majerczyk: Transcript of Proceedings – Sentencing, at 24, 32 *United States v. Edward J. Majerczyk*, No. 1:16-CR-00550-1 (N.D. Ill. Jan. 17, 2018), ECF 28 (imposing nine month sentence); (2) Herrera: Judgment in a Criminal Case, *United States v. Emilio Herrera*, No. 1:17-CR-0075-1 (N.D. Ill. March 28, 2018), ECF 17 (imposing three-year sentence); and (3) Garofano: Plea Agreement, *United States v. Garofano*, No. 3:18-CR-00038-VAB (D. Conn. April 11, 2018), ECF 9 (defendant pled guilty and was awaiting sentence at the time this article was submitted for publication).

32. Collins Press Release, *supra* note 30.

33. Exhibit to Transfer Document (Stipulation re. Factual Basis for Guilty Plea), *United States v. Ryan Collins*, No. 1:16-CR-0121-01 *at passim* (M.D. Pa. May 9, 2016), ECF 3-2.

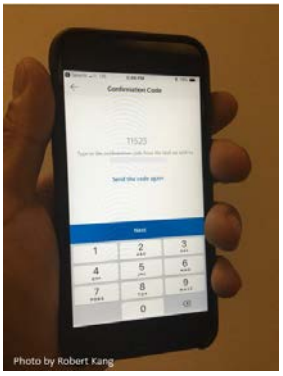
34. *Id.*

35. Judgment in a Criminal Case, *United States v. Collins*, *at* 1, No. 1:16-CR-0121-01 (M.D. Pa. Oct. 26, 2016), ECF 27.

Herrera of Chicago, Illinois; and George Garofano of Northford, Connecticut.[36] Still, there may be more and the hunt continues.

Part 2 Tips:

- Phishing emails are everywhere; don't take the bait. Modern phishing emails are more sophisticated than Collins' efforts, and often look like emails from banks or social media sites. View unsolicited emails asking for your password or other account information with suspicion. But even if you decide to change a password, don't click on any links within the email. Instead, go to the account website and change the password directly.



- Use multi-factor authentication, where available, to log into your accounts where available. Many online services allow users to add an additional step before logging into an account, such as the use of a unique code sent to the user's phone at the time of login. It's a minor inconvenience that is worth the extra safety.

- Use long, strong passwords. Want some tips? Play this simple password game developed by professors of computer science at Carnegie Mellon University.[37] The results may surprise you.

Part 3: Protecting Yourself From Other Hacking Methods (Working With Law Enforcement)

Starting this article with celebrity hacks may give the impression that the criminal justice system only moves for the rich and famous. In fact, while celebrity hacks attract media attention, they represent only a fraction of successfully prosecuted sex-based cybercrimes.

Assistant United States Attorney Lisa Feldman explains. A career cyber prosecutor with the United States Attorney's Office for the Central District of California, Feldman and her colleagues are at the forefront of catching and prosecuting cyber criminals.[38]

---

36. *See* sources cited, *supra* note 31.

37. The Password Game, Carnegie Mellon University, *available at* https://www.surveygizmo.com/s3/2758757/The-Password-Game-Carnegie-Mellon-University-website (last visited May 9, 2018).

38. The author is personally associated with Ms. Feldman and has discussed cybercrimes

"We're talking about the Chaney [celebrity] hacking case," notes Feldman who worked on the case. "But most of the victims we work with aren't celebrities. They're regular people. And we put the same effort into prosecuting those cases as we do the celebrity cases."[39] These aren't empty words: police and prosecutors have racked wins against sex-based cyber criminals across the nation from California to Florida.[40]

Feldman shares the sobering reality that many crimes go unreported, however. She cites the arrest and conviction of Luis Mijangos as an example.[41] At the time of his arrest, Mijangos was a 31-year-old man living in Santa Ana, California.[42] But where Chaney and Collins primarily collected intimate photos and emails, Mijangos engaged in "sextortion" – an especially malign, interactive type of cybercrime.[43] For example, in addition to harvesting intimate photos, Mijangos, a more skillful hacker than Chaney and Collins, would control the webcams built into his victims' computers and use them to photograph women in their private moments.[44] Mijangos would then contact the women to blackmail them into sending him even more nude photos.[45] "I never knew if it was someone that I knew or if it was a complete stranger [who attacked me,]" recounted one victim – identified only as "SG" – during the sentencing portion of Mijangos' eventual prosecution. "It would be in the back of my mind no matter where I went or who I went with. It was always there."[46]

Mijangos came to law enforcement's attention after one of his victims reported his crime.[47] The FBI caught Mijangos after backtracking though some

---

with her over several years. Quoted with permission ("Feldman Discussions").

39. *Id.*

40. *E.g.*, *Case o' The Week: The First and the Ninth – Osinger, First Amendment, and Internet Stalking*, Ninth Circuit Blog (June 14, 2014), at https://circuit9.blogspot.com/2014/06/case-p.html (California conviction); FBI, *Sextortion – Help Us Locate Additional Victims of an Online Predator* (July 7, 2015), at https://www.fbi.gov/news/stories/sextortion (Florida conviction)("FBI Sextortion Article").

41. Complaint for Violation of Title 18, United States Code, Section 875(d)(Extortion), *United States v. Mijangos*, No. CR10-743 GHK (C.D. Cal. June 17, 2010), ECF 1 ("Mijangos Complaint").

42. FBI Press Release, *Orange County Man Suspected of Hacking Computers Arrested on Federal charges Related to Demands for Sexually Explicit Videos from women and Teenage Girls* (June 22, 2010), *at* https://archives.fbi.gov/archives/losangeles/press-releases/2010/la062210a.htm.

43. *Id.* The GQ reporter who reported on Christopher Chaney also wrote an in-depth article about Luis Mijangos, David Kushner, *The Hacker is Watching*, GQ (Jan. 11, 2012), at https://www.gq.com/story/luis-mijangos-hacker-webcam-virus-internet ("Mijangos GQ Article").

44. *Id.*

45. *Id.*

46. Transcript of Sentencing, at *27-*28, *United States v. Luis Mijangos*, No. CR10-743 GHK (C.D. Cal. Dec. 13, 2011), ECF 96 ("Mijangos Sentencing Transcript").

47. Mijangos GQ Article, *supra* note 43.

of the emails he sent to that victim to online domains registered in his name.[48] But the horror is that Mijangos' computers showed he had victimized over 200 people, including over 40 kids.[49] None – of the underage victims reported the crime to law enforcement.[50] Why?

"They're young," said Feldman, as she recounted the reasons kids hesitate to report such crimes. "They are often afraid their parents will find out. They might also be scared to tell people they've been victimized. They may blame themselves. And criminals like Mijangos know how to exploit that fear and threaten their victims into keeping quiet. It's really scary for them. But we hope they tell us, so we [law enforcement] can help them."[51]

Feldman understands the difficulty that victims and survivors face in reporting sex-based crimes and tries to help members of the public understand their options before disaster strikes. In addition to comforting individual victims, Feldman teaches safe cybersecurity habits, in her spare time, to the public.[52] It's a form of community outreach intended to build trust between the public and law enforcement. Her audiences intentionally include schoolchildren and their parents.[53]

Feldman isn't alone. Many of her colleagues – including those in senior leadership – similarly volunteer their time. Tracy Wilkison, the First Assistant United States Attorney for the Central District of California (the second-highest ranking prosecutor in the District), shared her motivations for volunteering: "Because cybercrimes can happen to anyone, it's important for us not only to vigorously investigate and prosecute the crime after it has happened, but to also reach out and teach prevention as widely as possible," said Wilkison.[54] "We are providing tips to better protect oneself, as well as spreading the word that law enforcement can be trusted to support and aid victims of cybercrimes. We understand how horrifically violated the victim can feel, and we work very hard

---

48. *Id. See also* Mijangos Sentencing Transcript, *supra* note 46, at *27-*28.

49. Mijangos GQ Article, *supra* note 43. *See also* Mijangos Complaint, *supra* note 41, at 10, *United Stqtes v. Luis Mijangos*, No. CR10-743 GHK (C.D. Cal. June 17, 2010), ECF 1 (search warrant attached to Complaint describing victims).

50. Cybersecuring Hollywood Part II, *supra* note 11.

51. Feldman Discussions, *supra* note 38; FBI Sextortion Article, *supra* note 40 (young victim "Ashely" explains why she tried preventing her parents from going to police because she feared going to jail for sending intimate photos to a sextortionist).

52. The author is personally familiar with Ms. Feldman's volunteer work, and has participated in some of them. *E.g.* Ashley Cullins, *UCLA to host cyber event*, The Daily Journal (Sept. 29, 2015) (reporting on a presentation called "Cybersecuring Hollywood Part II," by Ms. Feldman, the author, and others. That presentation provided many of the same tips presented in this journal article).

53. *Id.*

54. The author is personally associated with Ms. Wilkison and has both discussed cybercrimes with her, and presented on cybercrimes to the public with her, over several years. Quoted with permission.

to help."[55]

Working with law enforcement requires courage on the part of a cybercrime survivor. But, as with the Chaney prosecution, the results of such cooperation can be powerful. In the Mijangos case, one of his victims, identified as "JM," explained why she overcame a clear fear of her attacker to work with law enforcement. [56] "He was threatening to ruin my work, to talk to my employers and send them pictures that he had personally grabbed also from my personal computer," she explained in court. "I would log onto work, he would somehow just pop up on my computer and call me a bitch . . . I started throwing up. I got a rash, developed a rash on my face, and I just couldn't go to work."[57] But JM found it important to stop Mijangos. "Prior to being a victim of this man, I was a victim of domestic violence," she told the judge, "and I would tell you that there is no difference [between the two.] And being so that I had just been a victim of [domestic violence] is why I decided to stand up to him."[58]

JM's message came through loud and clear. In 2011, the judge sentenced Mijangos to six years in prison.[59]

Part 3 Tips:

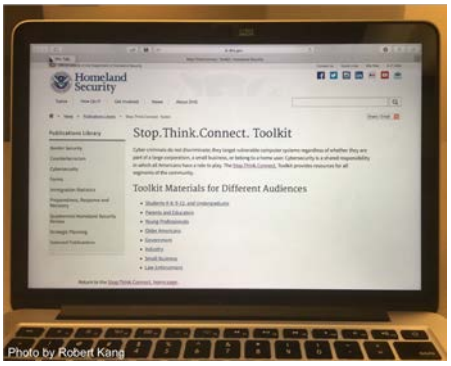
- Contact law enforcement if you believe you were the victim of a crime. Encourage your friends and loved ones, who may have been victimized, to do the same. Anyone can be a victim, even celebrities who may be someone's personal hero. Stars like Olstead and Johansson found the courage to share their stories publicly, and their courage contributed to the long sentence that shackles Chaney. Mijangos was convicted after a survivor found the strength to report the crime and work together with law enforcement.

- Cover your computer's built-in webcam when not in use. Sophisticated hackers like Mijangos can use it to take photos, even when the camera looks like it's off.

- Learn more about protecting online data. This article only touches the surface of available defenses. The United States Department of

55. *Id.*
56. Mijangos Sentencing Transcript, *supra* note 46, at *31-*32 ("JM" Victim Impact Statement).
57. *Id.*
58. *Id.*
59. *Id.* at *75 (judge issues sentence).

Homeland Security, in particular, has created cybersecurity guides geared towards protecting people from all walks of life, from children to business executives. (LINK – DHS Guides).[60]



Final Takeaways

Our online accounts represent a treasure trove of intimate information, both business and personal. Law enforcement has scored big wins in capturing and prosecuting offenders. But the first line of defense—the "human firewall"—rests with each of us. Completely protecting oneself from cyber criminals is a tough job. But it is possible to reduce the risk of becoming low hanging fruit by learning how to protect yourself against the methods employed by hackers like Chaney, Collins and Mijangos. And share the courage shown by survivors such as SG, JM, Renee Olstead and Scarlett Johansson, with others. Their testimony may inspire other survivors of cybercrime to contact law enforcement.

Acknowledgements:

Many law enforcement officers and government officials have generously given their time and energy to teach me and others about privacy and cybersecurity. I reference some of them here. Thank you: your dedication to protecting the public makes this nation a better place.

(In alphabetical order)

- **Gabriel Andrew**s, Supervisory Special Agent (FBI)
- **Rouman Ebrahim**, Deputy District Attorney (Los Angeles County District Attorney's Office)
- **Justin Feffer**, Lieutenant (Los Angeles County District Attorney's Office)
- **Lisa Feldman**, Assistant United States Attorney (United States Attorney's Office)
- **Hon. Wesley Hsu**, Judge & former federal prosecutor (Los Angeles County Superior Court)

---

60. United States Department of Homeland Security, Stop.Think.Connect.Toolkit, *at* https://www.dhs.gov/stopthinkconnect-toolkit (last visited May 10, 2018).

- **Gina Osborn**, Assistant Special Agent in Charge (FBI)
- **Michael Sohn**, Supervisory Special Agent (FBI)
- **Daniel Sutherland**, Associate General Counsel (United States Department of Homeland Security)
- **Gabriel Taran**, Assistant General Counsel (United States Department of Homeland Security)
- **John Tran**, Lieutenant Colonel (California Air National Guard)
- **Justin Vallese**, Supervisory Special Agent (FBI)
- **Steven Wang**, Deputy District Attorney (Los Angeles County District Attorney's Office)
- **Ryan White**, Chief – Cybercrimes and Intellectual Property Crimes Section Unit (United States Attorney's Office)
- **Tracy Wilkison**, First Assistant United States Attorney (United States Attorney's Office)