COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE FEDERAL TRADE COMMISSION

In the Matter of Craig Brittain

"FTC File No. 132 3120"

March 2, 2015

By notice published on February 6, 2015, the Federal Trade Commission ("FTC") has requested public comments on a Proposed Consent Order with Craig Brittain that would settle two alleged "violations of the FTC Act."[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that the final order adequately protects the privacy of individuals who are the subjects of cyberstalking apps and "revenge porn" internet businesses.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[2] The FTC's recent settlement with Snapchat arose from an FTC

[1] "Craig Brittain, Individually; Analysis of Proposed Consent Order To Aid Public Comment," 80 Fed. Reg. 25, 6714 (Feb. 6, 2015), *available at* http://www.ftc.gov//system/files/documents/federal_register_notices/2015/02/150206craigbrittainfrn.pdf.

[2] *See, e.g.,* Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by direct marketing industry), https://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), https://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief), https://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

complaint that EPIC filed in May 2013.[3] EPIC has also filed complaints regarding Facebook's acquisition of the messaging service WhatsApp;[4] Google's acquisition of the smart thermostat Nest;[5] and most recently, Facebook's emotional manipulation study.[6] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and October 24, 2011 subsequent settlement concerning the social networking service.[7] The Commission's settlement with Facebook also followed from a Complaint filed by EPIC and a coalition of privacy and civil liberties organizations in December 2009 and a Supplemental Complaint filed by EPIC in February 2010.[8]

In this case, the Respondent, Craig Brittain, operated several for-profit revenge porn websites. According to the FTC investigation, the Respondent "deceptively solicited photographs from individuals of themselves with their intimate parts exposed by misrepresenting that he would use such photographs solely for his personal private use."[9] The FTC further found, "Respondent unfairly disseminated photographs of individuals with their intimate parts exposed, along with personal information about them, for commercial gain and without the subject's

[3] EPIC: EPIC's Snapchat Privacy Complaint Results in 20-year FTC Consent Order (May 8, 2014), https://epic.org/2014/05/epics-snapchat-privacy-complai.html.
[4] In the Matter of Whatsapp, Inc., (2014) (EPIC & Center for Digital Democracy Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/ftc/whatsapp/WhatsApp-Complaint.pdf.
[5] In the Matter of Whatsapp, Inc., (2014) (Supplemental Materials in Support of Pending Complaint . . . Related Commentary Concerning Commission's Surprising Expedition of Google-Nest Review), https://epic.org/privacy/internet/ftc/whatsapp/WhatsApp-Nest-Supp.pdf.
[6] In re Facebook, Inc., (Psychological Study) (2014) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/ftc/facebook/Facebook-Study-Complaint.pdf.
[7] Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), http://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched").
[8] In the Matter of Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; In the Matter of Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request forInvestigation and for Other Relief), https://epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf; In the Matter of Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.
[9] FTC, *supra* note 1.

knowledge or consent, despite the fact that he knew or should have known that the individuals had a reasonable expectation their image would not be disseminated in that manner."[10]

EPIC supports the Consent Order in this case. The Order represents the FTC's first enforcement action against an operator of a revenge porn website and contains important privacy and security protections for victims of revenge porn. For instance, the Order prohibits the respondent and his business affiliates from engaging in further dissemination of revenge porn and requires respondent to destroy such content and personal information within 30 days of the order's effective date.[11] The Order also furthers the FTC's important work in identifying and prosecuting businesses that misappropriate images of people and sell those images to third parties for purposes to which the image subject did not consent.

However, because of the particularly egregious privacy violations at issue in this case and the steady growth of the revenge porn industry in the United States, EPIC believes that additional protections are needed. Specifically, EPIC urges the FTC to (1) pursue other operators of revenge porn sites; (2) remain vigilant of emerging web and mobile applications that facilitate spying and stalking via facial recognition technologies; and (3) further investigate– perhaps in a workshop format – the growing trend of companies recontextualizing images, for profit, without the knowledge or consent of the image subject.[12]

---

[10] FTC, *supra* note 1.

[11] In the Matter of Craig Brittain, FTC File No. 132 3120 (2014) (Agreement Containing Consent Order, http://www.ftc.gov/system/files/documents/cases/150129craigbrittainagree.pdfhttp://www.ftc.gov/system/files/documents/cases/150129craigbrittainagree.pdf (hereinafter "Brittain Proposed Consent Order").

[12] My EX Get Revenge, www.myex.com (disseminating sexual photos of individuals along with personally identifying information without consent of the subject); Anon-IB, http://anon-ib.ch/ (disseminating sexual photos of individuals without consent of the subject. Photos can be searched by city, state, and zip code as well as categories such as "ExGF" and "CollegeBitches") (last visited Feb. 12, 2015); Maxim Alter & Chris Riva, *9 creepy apps to watch out for: Swarm, Stalker, Crush, Wingman, NameTag, Breakup, Girls Around Me*, ABC News (May 23, 2014), http://www.newsnet5.com/news/9-creepy-apps-to-watch-out-for-swarm-stalker-crush-wingman-nametag-breakup-girls-around-me (listing nine cyberstalking apps that reveal name, location, images and other personal data of individuals to strangers in ways that are highly out of context and deeply disturbing).

In the case of Craig Brittain, EPIC recommends one addition. The consent order should expand the prohibited conduct to also include disseminating without consent photos or video that do not contain nudity but are still sexually suggestive or explicit.

I. The Commission should Pursue other Operators of Revenge Porn sites

While the settlement against Craig Brittain marks a milestone for the FTC, as its first revenge porn enforcement action, revenge porn websites continue to operate with impunity, taking advantage of patchwork state law bans and the Communications Decency Act's § 230 immunity.[13] EPIC recommends that the FTC pursue other websites and website operators of revenge porn websites, such as myex.com and anon-ib.ch.[14] These websites disseminate involuntary pornography and induce vicious cycles of harassment and privacy violations akin to rape.[15] The FTC is uniquely positioned to address this vexing problem of revenge porn by shutting down these websites and pursuing enforcement actions against their operators and business affiliates.

A. Revenge Porn is "involuntary pornography" and "cyber rape" [16]

Operators of revenge porn websites traffic in cyber rape. They betray consumers' expectation that the personal information they share confidentially will not later be disclosed in a drastically different context and exploited by third parties for commercial gain.[17] The Respondent's public disclosure of people's private images violated the context in which the

[13] *See infra* note 23.
[14] *See supra* note 12.
[15] *See* Corbin, *supra* note 17.
[16] End Revenge Porn, "What is Revenge Porn," http://www.endrevengeporn.org/welcome/ (last visited Feb. 20, 2015) (defining revenge porn as "a form of sexual abuse involving the distribution of nude/sexually explicit photos and/or videos of an individual without their consent"); Danielle Keats Citron & Mary Ann Franks, *Criminalizing Revenge Porn: Frequently Asked Questions*, 49 WAKE FOREST L. REV 345, 346 (May 19, 2014), *available at* file:///Users/epicipiop/Downloads/SSRN-id2368946.pdf (defining revenge porn as "involuntary pornography" and "cyber rape").
[17] *See* Danielle Citron and Woodrow Hartzog, *The Decision that Could Finally Kill the Revenge Porn Business*, The Atlantic (Feb. 3, 2015), http://www.theatlantic.com/technology/archive/2015/02/the-decision-that-could-finally-kill-the-revenge-porn-business/385113/ ("the collection of personal information is not devoid of context").

photos were originally taken and privately shared. Leading privacy scholar Danielle Citron has commented that the FTC's complaint focused on an aspect of revenge porn that has been largely "overlooked or minimized – the confidential relationships in which intimate images are shared."[18]

The contextual nature of a person's consent needs to be recognized.[19] The FTC should clarify that "information shared in confidential relationships deserves protection."[20] Revenge porn websites cause substantial and largely un-rectifiable reputational, financial, physical and emotional harm, the victims do not consent and have no reliable way of getting their personal information back once disseminated.[21]

B. The FTC is Uniquely Situated to Reverse the Revenge Porn Trend

The FTC can have a significant impact in the battle against revenge porn and cyberstalking. While some states have enacted revenge porn laws, many states have not.[22] The states that do often do not provide the strength of protection necessary to address this problem.[23]

---

[18] Citron & Hartzog, *supra* note 14.
[19] *See* Cyber Civil Rights Legal Project, http://www.cyberrightsproject.com/ ("people have a right of privacy in their intimate photographs and videos, and . . . the public, online dissemination of that media without consent is an invasion of that sexual privacy amounting to a 'cyber civil rights' violation").
[20] Citron, *Hate Crimes in Cyberspace*, 146-148, Harvard University Press (2014).
[21] *See* Citron & Franks*, supra* note 22 at 347; Cyber Civil Rights Initiative, *A message from our founder, Holly Jacobs* (Oct. 6, 2013), http://www.cybercivilrights.org/a_message_from_our_founder_dr_holly_jacobs (describing the aftermath of being a revenge porn victim as "[full-time] damage control" while "continuing to be shamed, silenced, striiped of monetary funds, and turned away"); Nina Bahadur, *Victims of Revenge Porn Open Up On Reddit About How It Impacted Their Lives,* Huffington Post (Jan. 10, 2014), http://www.huffingtonpost.com/2014/01/09/revenge-porn-stories-real-impact_n_4568623.html (listing five harms victims report experiencing: "humiliation," "concern for personal safety," "need for hypervigilance," "fear of being watched," and "body shame"); Ave Mince-Didier, *Revenge Porn: Laws & Penalties*, Criminaldefenselawyer.com, http://www.criminaldefenselawyer.com/resources/revenge-porn-laws-penalties.htm (last visited Feb. 20, 2015) ("Images can also be easily picked up by other websites, and content that is widely distributed on the Internet is difficult to remove. So, even if a person succeeds in getting images removed from one site, it may be difficult or impossible to get them completely off the Internet").
[22] C.A. Goldberg Law, States with Revenge Porn Criminal Laws, http://www.cagoldberglaw.com/states-with-revenge-porn-laws (last updated Jan. 1, 2015) (listing 16 states that have passed revenge porn laws).
[23] *See e.g.*, Eric Goldman, *California's New Law Shows It's Not Easy to Regulate Revenge Porn,* http://www.forbes.com/sites/ericgoldman/2013/10/08/californias-new-law-shows-its-not-easy-to-regulate-revenge-porn/ ("In sum, California's new revenge porn law only covers one category of involuntary porn," failing to apply to

Many of the states with these laws classify the distribution of sexually explicit images without the subject's consent as a misdemeanor, rather than a felony.[24] This sends the message that being the victim of a revenge porn attack is not very serious and does not cause severe harm. Furthermore, the nature of the privacy harm discourages victims from seeking aide from the police.[25] Victims who alert the police that they have been the subject of an attack are subjected to more attention, less privacy, and the potential of further disseminating the harmful content. Victims are substantially harmed by online and offline shaming, and it affects their careers, relationships, and sense of self.[26] This is a serious problem. It is endemic, not isolated, and needs to be swiftly addressed by the full force of the FTC's enforcement powers.

II. The Commission should Examine Emerging Business Practices that Facilitate Spying and Stalking via Facial Recognition

As the industry of facial recognition technologies expands, the FTC must be watchful of web and mobile applications that provide tools to spy on and stalk people.[27] Many mobile applications allow users to see, in real time, the social media profiles of strangers around them.[28] Pairing facial recognition with publicly available social media profiles and photos, a user may,

website and mobile operators, hackers, and anyone who cannot be proven to have intended to inflict the requisite amount of emotional distress).

[24] C.A. Goldberg Law, *supra* note 31.

[25] Citron, *supra* note 26, 19 ("Despite the gravity of their predicaments, cyber harassment victims are often told that nothing can or should be done about online abuse. Journalists, bloggers, lay observers, and law enforcement officials urge them to ignore it").

[26] Marlisse Sweeney, *What the Law Can (and Can't) Do About Online Harassment,* The Atlantic (Nov. 12, 2014), http://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/ (discussing the dire consequences of cyber harassment and cyberstalking).

[27] *See* Quentin Fottrell, *5 Apps for Spying on your Spouse,* Market Watch (Jan. 31, 2015), http://www.marketwatch.com/story/5-apps-for-spying-on-your-spouse-2014-03-10 (listing 5 popular spyware apps); Aarti Shahani, *Smartphones Are Used to Stalk, Control Domestic Abuse Victims,* NPR (Sept. 15, 2014), http://www.npr.org/blogs/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims (describing how spyware apps aid domestic abuse); Alter & Riva, *supra* note 20.

[28] NameTag, http://www.nametag.ws/ (last visited Feb. 23, 2015) ("NameTag links your face to a single, unified online presence that includes your contact information, social media profiles, interests, hobbies and passions"); Liz Klimas, *Creepy 'Girls Around Me' App Pulled- But Privacy Discussion Continues,* The Blaze (Apr. 3, 2012), http://www.theblaze.com/stories/2012/04/03/girls-around-me-app-creepily-identified-nearby-women-pulled-from-app-store-but-privacy-discussion-continues/ (discussing the 2012 geo-location tracking app that showed users photos of people nearby).

with the touch of a button, learn the name, age and other personal information of those who happen to be within range of the user's mobile device.[29] These types of applications are more than merely creepy; they expose unsuspecting individuals to the constant threat of being stalked or harassed, online and in real life. The consequences of being a victim of cyberstalking and cyber harrassment, as with revenge porn, are serious and long lasting, affecting the victims' professional and personal relationships in damaging and irreversible ways.[30]

EPIC urges the FTC to monitor the privacy practices of web and mobile applications employing facial recognition software. Privacy by design in this area is critical, yet apps fall short of providing basic protections. For example, the facial recognition app NameTag forces individuals to opt-out of rather than opt-in to its service.[31] If an individual does not affirmatively opt-out, his or her face may be scanned for personal information by anyone using this application.[32] Such inherently secretive and invasive applications cannot fairly shift the burden to the targets of facial recognition scans to opt out of the use of such software on them. [33] Doing so

[29] Nametag, About, http://www.nametag.ws/ (last visited Feb. 23, 2015) ("Using the NameTag smartphone or Google Glass app, simply snap a pic of someone you want to connect with and see their entire public online presence in one place"); Girls Around Me, girlsaround.me (last visited Feb. 23, 2015) ("This foursquare-based tool helps you see where nearby girls are checking in, and shows you what they look like and how to get in touch!").
[30] Sheryl Ubelacker, *Cyberstalking: Trauma Even More Intense Than In-Person Harassment: Expert,* Huffington Post (Aug. 6, 2011), http://www.huffingtonpost.ca/2011/08/06/trauma-from-cyberstalking-more-intense_n_920088.html (quoting Dr. Elizabeth Carll's presentation to the American Psychological Association, "The symptoms of harassment and e-harassment are very similar – anxiety, fear, nightmares, feelings of helplessness, hypervigilence, having eating and sleeping difficulties, feeling out of control, a loss of personal safety – all of those kind of things go with harassment. . . But what's different is that it is more intense because the electronic harassment is so much more pervasive. Whatever humiliating thing they want to say about you can go out to everybody and they can continue to do this wherever you are, if you're online").
[31] NameTag, Opt Out of NameTag, http://www.nametag.ws/optout/ (last visited Feb. 23, 2015)(requiring individuals who wish to opt-out to nevertheless create a NameTag profile)
[32] *See* NameTag, *supra* note 39 ("With NameTag, your photo shares you. Don't be a stranger"); Charles Poladian, *Facial Recognition Apps, Like NameTag, Could Lead to A Situation Like the 'War on Terror,'* International Business Times (Feb. 4, 2014) (quoting Iowa State University professor Brian Mennecke, "The challenge is that when these applications are released for public use, the potential for abuse is great because it will be virtually impossible to opt out").
[33] Letter From Sen. Al Franken to FacialNetwork.com (Feb. 5, 2014), *available at* http://www.franken.senate.gov/files/letter/140205NameTagLetter.pdf ("Unlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a distance, without the knowledge or consent

is an ineffective privacy safeguard, wholly inadequate when dealing with nonconsensual image re-appropriation.

EPIC previously urged the Federal Trade Commission to suspend the use of facial recognition techniques by businesses pending the establishment of adequate privacy safeguards.[34] EPIC explained, "Consumers today enjoy enormous freedom and personal safety because they are able to interact with so many merchants, who are essentially strangers, without concern that they will be secretly tracked and profiled. It is critical that the Federal Trade Commission take affirmative steps to ensure the protection of the consumers' right to safeguard their identity."[35] EPIC also emphasized the importance of the right to anonymity, including the right to choose when to be anonymous. Instead of establishing privacy safeguards, the Commission chose instead to release a list of best practices for companies developing facial recognition software and applications. The report recommended that companies design facial recognition programs with consumer privacy, security, and contextual use in mind.[36]

In light of new concerns about the misuse of facial recognition techniques to stalk and harass individuals, EPIC again renews its recommendation that the Commission formally block further deployment of facial recognition techniques in business practices until adequate safeguards are established.

---

of the person being identified. Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere")

[34] EPIC, *Comments to the Federal Trade Commission on Face Facts: A Forum on Facial Recognition* (Jan. 31, 2012), https://epic.org/privacy/facerecognition/EPIC-Face-Facts-Comments.pdf.

[35] *Id*. at 1.

[36] Federal Trade Commission Staff Report, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies (October 2012), http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf; Press Release, *FTC Recommends Best Practices for Companies that Use Facial Recognition Technologies,* Federal Trade Commission (Oct. 22, 2012), http://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition.

III. The Commission should Investigate Businesses that Appropriate Images of People without their Knowledge and Consent

As EPIC recently explained in a case concerning the misappropriation of images for advertising purposes, the cornerstone of modern privacy law is the right and ability of an individual to control when and whether their likenesses will be used by another for commercial benefit.[37] The law recognizes the importance of these rights and through the tort of misappropriation and the right of publicity provides legally actionable grounds for protecting them.[38] The Commission should defend this right and ability by investigating the trend of businesses misappropriating images of people without their knowledge or consent – including those businesses engaged in revenge porn.

The right and ability to control the commercial use of images of one's likeness has roots in early New York state invasion of privacy case law in the seminal case of *Roberson v. Rochester Folding Box Company*, 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902).[39] The *Roberson* case was the genesis for New York's statutory protection of a person's right to control the commercial use of their image or likeness, and holds anyone that violates this right without consent guilty of a misdemeanor.[40] Since New York's enactment of NY Civil Right Law § 50, the protection of such rights has gained widespread acceptance across the nation.[41] In fact, as EPIC's amicus brief

[37] Brief for Electronic Privacy Information Center as Amicus Curiae Supporting Appellants at 2, Angel Fraley, et al. v. Facebook, Inc., No. 13-16918 (9th Cir. Feb. 20th, 2014); *See also,* Restatement (Second) of Torts §652(C) (1977)*, and* Restatement (Third) of Unfair Competition §46 (2006).
[38] Brief Supporting Appellants at 2.
[39] *Id. at 3*; Roberson v. Rochester Folding Box Company, 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902).
[40] *Id. at 4 – 5; NY Civil Rights Law § 50 (McKinney).*
[41] Amicus Brief Supporting Appellants at 5; *See also, e.g.,* N.C. Gen. Stat. Ann. § 66-152 (West); VA Code Ann. § 59.1-336; Or. Rev. Stat. Ann. § 646.465 (West); Ala. Code § 8-27-3; Alaska Stat. Ann. § 45.50.910 (West); Ohio Rev. Code Ann. § 1333.61 (West).

points out, "[s]ince this first statute was enacted, over half of all states have recognized a right of publicity".[42]

In the Facebook matter, EPIC argued that the company's use of user images in "Sponsored Stories" advertising campaigns violated the right and ability of these users to control whether their likenesses are used for commercial benefit, and that any settlement agreement that allowed them to do so would be in direct contravention of state law covering the same conduct and subject matter.[43] Similarly, the conduct of the businesses involved in the revenge porn industry also violate the right and ability to control whether an individual's likeness is used for commercial benefit. As in the case of Facebook's Sponsored Stories, the privacy harm results from the fact that revenge porn victims do not consent to the dissemination of their images.

The Commission has recognized the work of states in crafting image-protective privacy laws.[44] In its amicus brief submitted in the *Fraley* case, the FTC argued that nothing in the Children's Online Privacy Protection Act ("COPPA"), or in its legislative history, indicated that Congress intended for COPPA to preempt state privacy laws relating to those who fall outside of COPPA's protections.[45] The FTC's position on COPPA preemption underscores the importance of the well-established state privacy laws governing privacy, "… that had existed [prior to COPPA] for nearly a century[,]"[46] and that the FTC should work to protect these laws by investigating those who violate them – like the businesses involved in revenge porn.

IV. The Commission should modify the Consent Order to Include Sexually Suggestive Images

[42] Brief Supporting Appellants at 5.
[43] Brief Supporting Appellants at 5 and 7 – 8.
[44] Brief for the Federal Trade Commission as Amicus Curiae Supporting Neither Party, Angel Fraley, et al. v. Facebook, Inc., No. 13-16918 (9th Cir. Mar. 20th, 2014)
[45] *Id at 1 and 8.*
[46] *Id at 11.*

The Proposed Order bans Respondent from further engagement in the revenge porn business.[47] Specifically, the Proposed Order states that Respondent is "permanently restrained and enjoined from disseminating, through a website or online service, a video or photograph of an individual with his or her intimate parts exposed without" first obtaining the subject's express written consent to do so and disclosing to the subject that such content will be distributed publicly for commercial gain.[48] EPIC supports this prohibition with the recommendation that the Commission add language expanding the prohibition to also include the nonconsensual dissemination of sexually graphic images and video of non-nude individuals. As is, the Proposed Order only speaks to nude or partially nude photos and video ("intimate parts exposed"). However, the nonconsensual dissemination of sexually suggestive images or video of fully or partially clothed individuals can be just as harmful and malicious.[49]

Illinois' recently passed an anti-revenge porn statute that addresses this concern.[50] Illinois' law bans the non-consensual distribution of images and videos depicting individuals engaged in a sex act, whether clothed or not, as well as the non-consensual distribution of images and videos showing partially exposed or transparently clothed "intimate parts."[51] There is no intent requirement and the law applies to anyone who disseminates the material and reasonably should have known that the material was personal and private and the dissemination non-

[47] Brittain Proposed Consent Order, *supra* note 19.
[48] *Id.*
[49] End Revenge Porn, *Seven Reasons Illinois is Leading the Fight Against Revenge Porn* (Dec. 31, 2004), http://www.endrevengeporn.org/seven-reasons-illinois-leading-fight-revenge-porn/ ("not all intimate sexual acts involve nudity").
[50] Illinois Criminal Code of 2012, 720 ILCS 5/11-23.5 (2015), *available at* http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=098-1138.
[51] *Id.* (defining "intimate parts" as "the fully unclothed, partially unclothed or transparently clothed genitals, pubic area, anus, or if the person is female, a partially or fully exposed nipple, including exposure through transparent clothing" and banning the "non-consensual dissemination of private sexual images" of individuals who are "engaged in a sexual act or whose intimate parts are exposed, in whole or in part").

consensual.[52] The law has been championed by experts in the field as the strongest state law yet against revenge porn.[53]

To effectively ban Craig Brittain and his business affiliates from the revenge porn business, the FTC should expand the prohibition against Craig Brittain and affiliates to include prohibiting the non-consensual dissemination of sexually suggestive images and video. EPIC recommends the FTC adopt the language of the Illinois state bill to include images or video depicting individuals engaged in sex acts as well as images or video revealing partially exposed or transparently clothed intimate parts.[54] These additions would provide further protection to potential future victims of Craig Brittain and would better serve the FTC's goal of sending a strong message to revenge porn website operators and other disseminators that revenge porn content encompasses more than just nude photos leaked online.[55]

V. Conclusion

EPIC supports the Consent Order in this case. However, revenge porn victims' privacy would be better protected – and better prevented – by modifying the Order to address the issues raised in these comments.

Respectfully Submitted,

[52] *Id.* ("(b) A person commits non-consensual dissemination of private sexual images when he or she: . . . (2) obtains the image under circumstances in which a reasonable person would know or understand that the image was to remain private; and (3) knows or should have known that the person in the image has not consented to the dissemination").
[53] Barbara Herman, *Illinois Passes Revenge Porn Law with Teeth,* International Business Times (Jan. 6, 2015), http://www.ibtimes.com/illinois-passes-revenge-porn-law-teeth-other-states-should-copy-says-privacy-lawyer-1774974; End Revenge Porn, *supra* note 57.
[54] *Supra* note 59.
[55] Herman, *supra* note 61 (quoting attorney and anti-revenge porn advocate Carrie Goldberg, "So much is said about how laws butt up against free speech, but if we lose the expectation of privacy in taking images meant only for someone we trust, then we lose another valuable form of speech: our private speech. There is nothing wrong with taking pictures of yourself that are meant only for another person you trust").

Marc Rotenberg,
EPIC Executive Director

Julia Horwitz, Director,
EPIC Consumer Privacy Project

Brooke Olaussen,
EPIC Consumer Protection Fellow
Electronic Privacy Information Center
1718 Connecticut Ave NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)