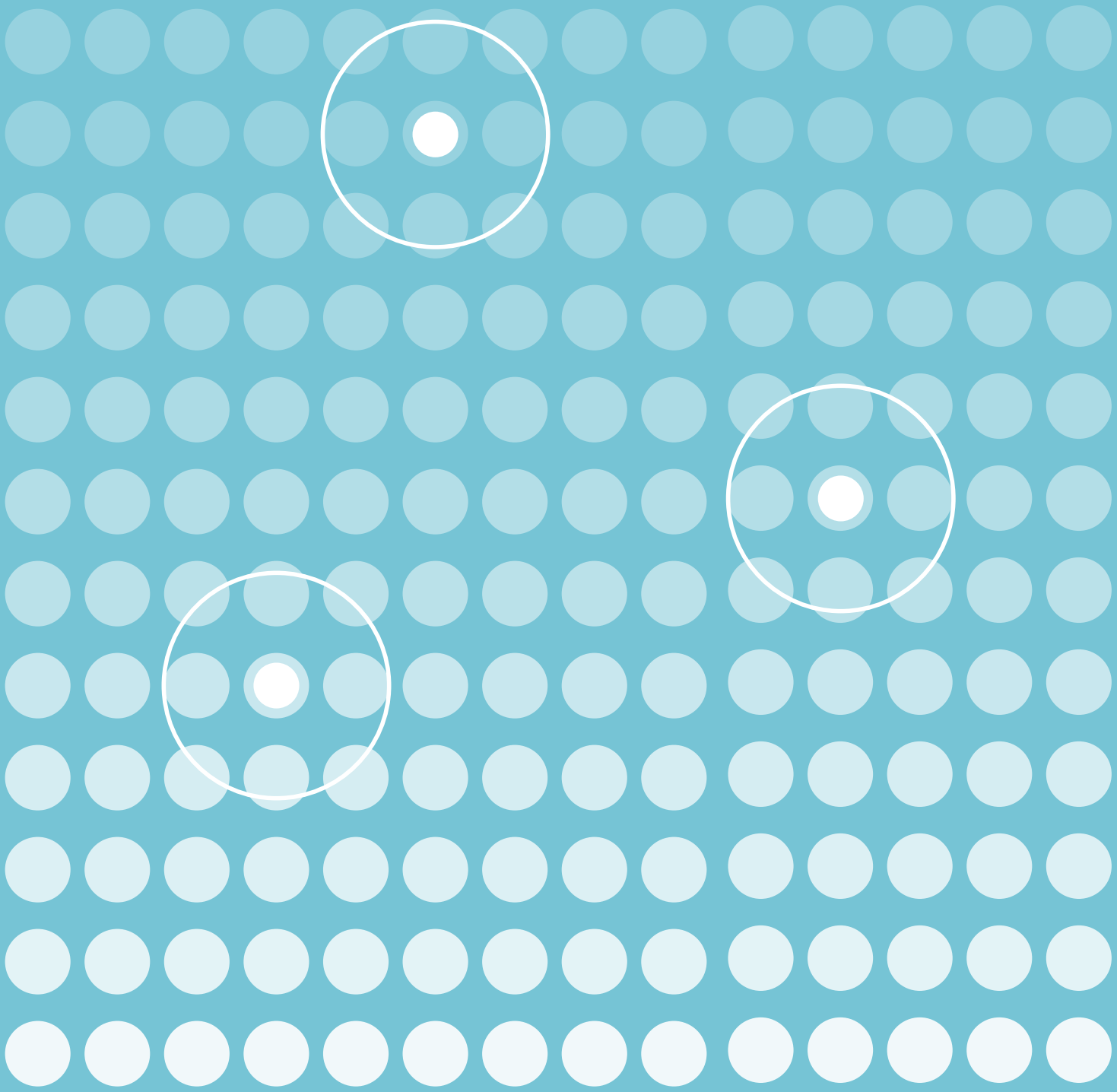
Data&Society RESEARCH INSTITUTE

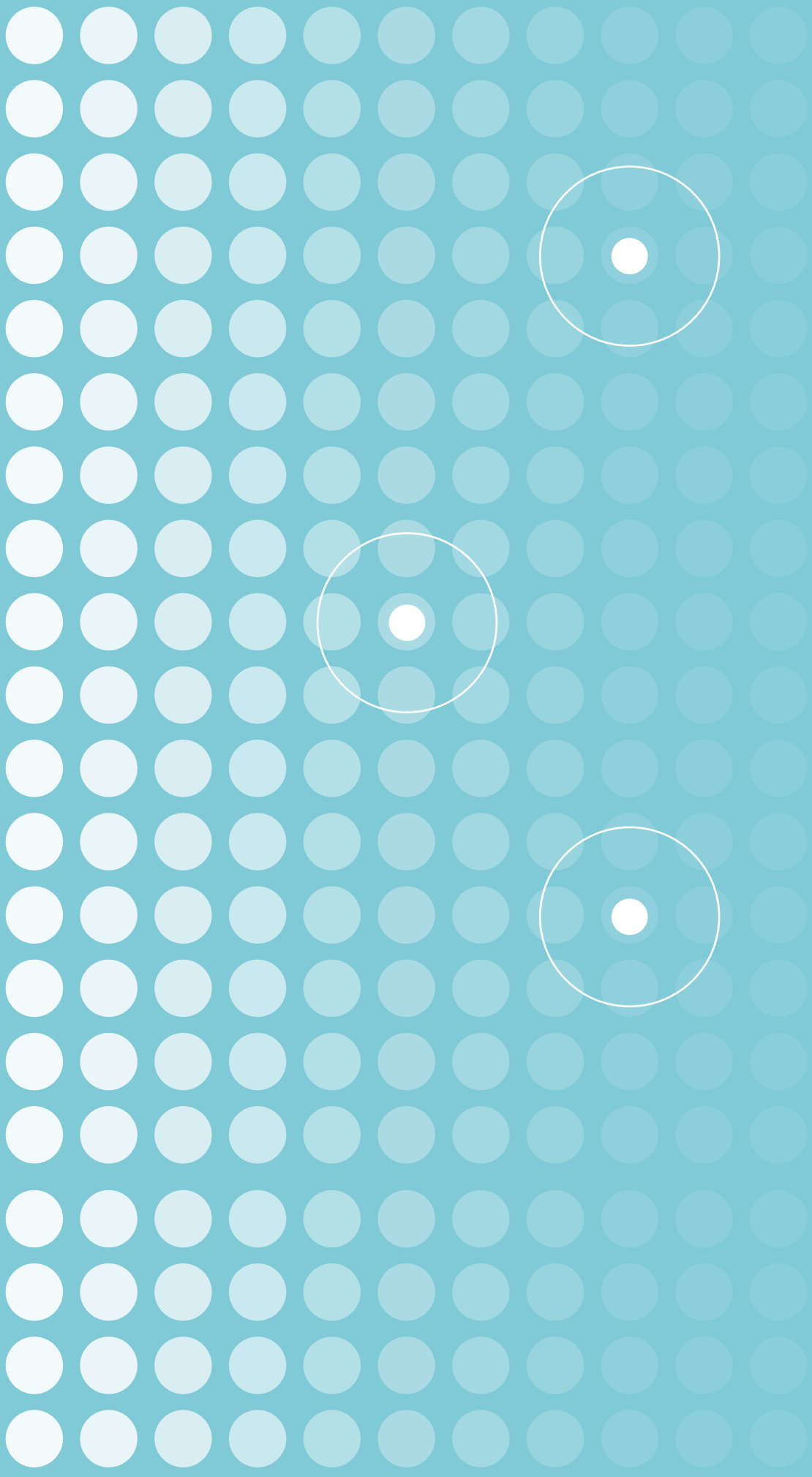
CiPHR Center for *Innovative* Public Health Research

NONCONSENSUAL IMAGE SHARING: ONE IN 25 AMERICANS HAS BEEN A VICTIM OF "REVENGE PORN"

Data Memo 12.13.2016

AMANDA LENHART, Data & Society
MICHELE YBARRA, Center for Innovative Public Health Research
MYESHIA PRICE-FEENEY, Center for Innovative Public Health Research





What is nonconsensual image sharing?

Nonconsensual image sharing, also commonly called "revenge porn," is when someone shows, sends, or posts nude or nearly nude photos or videos of someone else without the consent of the person pictured.[1] In some cases, the images are created consensually, such as when romantic partners take pictures for each other or together.[2] In other cases, these images may be created nonconsensually, such as when someone is secretly or forcibly photographed or taped. These images are also posted online in different ways. Images are sometimes posted by a romantic partner in the aftermath of a break up or during a fight, or may be obtained by someone hacking into a private online space and stealing the images. In all cases, these sensitive images are shared with third parties without the consent of the person pictured.

In 2014, nonconsensual image sharing made headlines when dozens of celebrities' private photos were exposed. An Illinois man published over 500 photos of celebrities (almost all of them women) that he had stolen from their email and online storage accounts.[3] He had obtained targets' login credentials through a series of phishing attacks over the course of almost a year. Victims of this hack included actresses, models, and athletes; many of the celebrities targeted have spoken out about the emotional distress they have experienced from this invasion of privacy.[4]

More recently, a Saturday Night Live castmember was targeted by hackers and trolls, who mounted a campaign of racist and sexist attacks against the comedian on social media.[5] Later, hackers stole private information from her online storage accounts—including nude photos and images of sensitive documents, such as her driver's license and passport. The hackers also compromised the comedian's private website, then published the stolen material and racist images on her site.[6] The exposure of her private materials was one component of a campaign of intimidation and retribution for speaking out against her previous harassment.[7]

---

1. The survey for this report specifically asked internet users about "nearly nude or nude photos or videos," but the term may also refer to non-nude images of the victim that are sexual or sensitive in nature.

2. In 2013, a Pew Research Center report found that 9% of adult cell phone owners in the U.S. had sent a nude or partially nude image of themselves to someone else, and 20% of cell owners said they had received such an image of someone they knew. A. Lenhart and M. Duggan. "Couples, the Internet, and Social Media." Pew Research Center: Internet, Science & Tech, February 11, 2014. http://www.pewinternet.org/2014/02/11/couples-the-internet-and-social-media/.

3. J. Serna. "Man Convicted of Hacking Gmail and iCloud Accounts of At Least 30 Celebrities in L.A." Los Angeles Times, September 28, 2016.http://www.latimes.com/local/lanow/la-me-ln-phishing-scam-conviction-20160928-snap-story.html.

4. F. Garcia, "iCloud celebrity nude leak: Man pleads guilty to hacking emails of stars including Jennifer Lawrence and Kate Upton. "The Independent, September 26, 2016.
http://www.independent.co.uk/news/people/icloud-celebrity-nude-leak-jennifer-lawrence-kate-upton-man-pleads-guilty-a7334031.html. Jennifer Lawrence discussed the incident in a 2014 interview with Vanity Fair: "Just because I'm a public figure, just because I'm an actress, does not mean that I asked for this. It does not mean that it comes with the territory. It's my body, and it should be my choice, and the fact that it is not my choice is absolutely disgusting," Lawrence said. "It is not a scandal. It is a sex crime. It is a sexual violation." Quoted in "Both Huntress and Prey," by S. Kashner. "Both Huntress and Prey." Vanity Fair, November 2014.
http://www.vanityfair.com/hollywood/2014/10/jennifer-lawrence-photo-hacking-privacy

5. K. Rogers. "Leslie Jones, Star of 'Ghostbusters,' Becomes a Target of Online Trolls." The New York Times, July 19, 2016. http://www.nytimes.com/2016/07/20/movies/leslie-jones-star-of-ghostbusters-becomes-a-target-of-online-trolls.html.

6. K. Rogers and J.E. Bromwich. "Hackers Publish Nude Pictures on Leslie Jones's Website." The New York Times, August 24, 2016. http://www.nytimes.com/2016/08/25/movies/leslie-jones-website-hacked.html?_r=0.; C. D'Zurilla. "Homeland Security Is Investigating Nude-Photo Cyberattack on Leslie Jones." Los Angeles Times, August 25, 2016.
http://www.latimes.com/entertainment/gossip/la-et-mg-leslie-jones-fbi-investigates-hacking-nude-pictures-20160825-snap-story.html.

7. J. Otterson. "Leslie Jones' Website Hacked: Nude Photos, Personal Info Exposed." TheWrap, August 24, 2016. http://www.thewrap.com/ghostbusters-star-leslie-jones-website-suffers-horrific-vandalism-by-hackers/.

The harms from nonconsensual image sharing can be substantial; a single act of posting sensitive images can cause lasting and ongoing reputational damage to victims. These images are often posted alongside personally-identifying information about the victim when they are posted in online spaces, which can lead to additional harassment and threats from third parties.[8] Even if the images are never actually posted publically, the perpetrator may use threats to post such images as a method of controlling or intimidating the victim.

Until recently, victims of nonconsensual pornography often faced difficulty pursuing legal action against perpetrators.[9] Some perpetrators and operators of "revenge porn" websites have been prosecuted under existing laws, such as the 1986 Computer Fraud and Abuse Act (CFAA), for hacking,[10] impersonation, identify theft, and extortion.[11] Legal scholar Amanda Levendowski has also written that because most of the images in question were originally taken by the victims themselves, they may be able to seek protection under copyright laws;[12] some victims have submitted takedown requests to websites under the 1998 Digital Millennium Copyright Act (DMCA).[13]

In response to the lack of specific criminal laws against nonconsensual pornography and a growing public awareness of the issue, more than 30 states have passed legislation over the past three years attempting to define and criminalize "revenge porn" and other types of nonconsensual pornography, according to George Washington Univeristy Law professor Orin Kerr.[14] While national legislation has yet to be passed, U.S. Representative Jackie Speier (D-CA) introduced a bill criminalizing revenge porn in mid-2016.[15]

One in 25 Americans has been a victim of threats or posts of nearly nude or nude images without their permission

Media coverage of revenge porn largely focuses on instances when celebrities have had private nude or explicit photos or videos made public without their consent, but this experience is not limited to the famous and newsworthy. Roughly 3% of all online Americans have had someone threaten to post nude or nearly nude photos or videos of them online to hurt or embarrass them, and 2% of online Americans have had someone actually post a photo of them online without their permission. Taken together, 4% of internet users—one in 25 online Americans—have either had sensitive images posted without their permission or had someone threaten to post photos of them.

---

8. D.K. Citron and M.A. Franks, "Criminalizing Revenge Porn." Wake Forest Law Review 49, 345 (2014).
9. One victim's accont of her experiences: A. Chiarini. "I was a victim of revenge porn. I don't want anyone else to face this," "The Guardian, November 19, 2013. https://www.theguardian.com/commentisfree/2013/nov/19/revenge-porn-victim-maryland-law-change.
10. For instance, revenge porn website operator Hunter Moore hired another man to hack into email accounts in order to steal nude photos to post on the site. One of the charges against them was for hacking (specifically "unauthorized access of a protected computer to obtain information") in violation of the CFAA. M. Masnick. "Revenge Porn 'King' Hunter Moore Indicted & Arrested; May Actually Be A Legitimate Use of CFAA."Techdirt, January 23, 2014. https://www.techdirt.com/articles/20140123/12202625969/revenge-porn-king-hunter-moore-indicted-arrested-may-actually-be-legitimate-use-cfaa.shtml.
11. Bollaert was also charged with extortion because he charged victims a fee of several hundred dollars to remove images of themselves that were posted to his website without their consent. L. Winkley and D. Littlefield. "Sentence Revised for Revenge Porn Site Operator." The San Diego Tribune, September 21, 2015. http://www.sandiegouniontribune.com/sdut-kevin-bollaert-revenge-porn-case-resentencing-2015sep21-story.html.
12. A. Levendowski. "Our Best Weapon Against Revenge Porn: Copyright Law?" The Atlantic, February 4, 2014. http://www.theatlantic.com/technology/archive/2014/02/our-best-weapon-against-revenge-porn-copyright-law/283564/.
13. C. Laws. "One Woman's Dangerous War Against the Most Hated Man on the Internet." Jezebel, November 22, 2013. https://jezebel.com/one-womans-dangerous-war-against-the-most-hated-man-on-1469240835.
14. O. Kerr. "The path of computer crime law." The Washington Post, October 13, 2016. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/13/the-path-of-computer-crime-law/.
15. M. Trujillo. "Revenge porn bill unveiled after struggle to bring tech on board." The Hill, July 14, 2016. http://thehill.com/policy/technology/287773-revenge-porn-bill-unveiled-after-struggle-to-bring-tech-on-board.

One in ten young women have been threatened with the possibility of public posting of explicit images

Among all online Americans, 3% have had someone threaten to post nearly nude or nude photos or videos of them online to hurt or embarrass them. These threats can be used to coerce or control individuals and can cause significant mental distress, even if the photos themselves are never shared with others or posted publically.

Young people ages 15-29 are the age group most likely to report being threatened with the potential sharing of nude or nearly nude images, with one in 14 (7%) internet users under the age of 30 experiencing this compared with 2% of adults ages 30 and older.[16] Young women in particular are more likely to be targeted: One in 10 women under the age of 30 have experienced threats of nonconsensual image sharing, a much higher rate than either older women or older and younger men.

Young adults are more likely than older adults to have had someone post an explicit photo without their permission; men and women are equally likely to have someone post a photo

About 2% of all online Americans have had someone post a nearly nude or nude photo of them online without their permission. Younger internet users, particularly those ages 18-29, are more likely than older adults to have had nude or nearly nude photos of themselves posted without permission (5% vs. 1%). At the same time, men and women are equally likely to have sensitive photos posted.

LGB internet users are far more likely than those who identify as heterosexual to have experienced threats of or actual nonconsensual image-sharing

Among internet users who identify as lesbian, gay, or bisexual (LGB), 15% say someone has threatened to share a nude or nearly-nude photo or video of them without their permission, a far higher rate than among heterosexual internet users (2%). In addition, 7% of LGB respondents have had someone share a nude or nearly nude image of them, compared with 2% of heterosexual internet users. Taken together, 17% of LGB Americans have either had an image shared without their consent or have had someone threaten to share an image of them.

Many victims of nonconsensual image sharing and related threats have had an account or computer hacked

Although we cannot say whether these incidents are necessarily related, 43% of those who have endured threats of the posting of nude photos or have had photos posted online also report that someone has hacked into their online account or computer and stolen sensitive personal information. This compares with 12% of those who haven't been threatened with or experienced the exposure of these images but who report similar hacking of their accounts or devices.

16. Notably, the minors in our sample (15-17 year-olds) are less likely to report these experiences than those ages 18 to 29.

Nonconsensual image sharing summary table

% among all internet users (n=3,002)

		Have had someone threaten to expose photos	Have had someone post photos	Total have had someone threaten and/or post photos
Total		**3**	**2**	**4**
Age and sex				
a	Men ages 15-29	3[cd]	4[cd]	6[d]
b	Women ages 15-29	10[bcd]	6[cd]	12[cd]
c	Men ages 30+	2	1	2
d	Women ages 30+	2	1	2
	Sex			
a	Men	2	2	3
b	Women	4[a]	3	5
Race/ethnicity				
a	White (non-Hispanic)	3	2	4
b	Black (non-Hispanic)	5[c]	5[a]	7
c	Hispanic	2	2	3
	Age			
a	15-17	3	3	4[de]
b	18-29	8[acde]	5[cd]	10[acde]
c	30-49	3[de]	2[d]	4[de]
d	50-64	<1	1	1
e	65+	<1	-	<1
Household income (among ages 18+)				
a	< $30,000	7[bcde]	4[cde]	8[cd]
b	$30,000 - $49,999	4[cd]	3[d]	8[cd]
c	$50,000 - $74,999	1	2	2
d	$75,000 - $99,999	1	1	1
e	$100,000+	2	1	3
Education (among ages 18+)				
a	Less than high school	3	5	6
b	High school graduate	3[d]	2	4
c	Some college	4[d]	4[bd]	5[d]
d	College graduate	2	1	2
Sexual identification				
a	LGB	15[b]	7[b]	17[b]
b	Heterosexual	2	2	3

Columns marked with a superscript letter ([a]) indicate a statistically significant difference at the 95% level between that row and the row designated by that superscript letter (within each subgroup).

Source: Data & Society / CiPHR Measuring Cyberabuse Survey, May 17- July 31, 2016. Interviews were conducted in English and Spanish (total n=3,002 U.S. internet users age 15 and older).

Resources for victims of nonconsensual image sharing

Below is a list of resources for those looking for information or assistance in handling nonconsensual pornography:

Without My Consent has educational materials and practical resources for victims of nonconsensual pornography, including a state-by-state guide explaining relevant laws for 10 states. **More: http://www.withoutmyconsent.org**

The Cyber Civil Rights Initiative is an advocacy organization that maintains a 24-hour Crisis Helpline for victims of nonconsensual pornography at 844-878-2274.
More: **https://www.cybercivilrights.org/**

The California Attorney General's office maintains a website on cyber exploitation with resources for victims, tools for law enforcement, and links to privacy and removal policies.
More: **https://oag.ca.gov/cyberexploitation**

Methods

The data for this study were collected through the Data & Society / CiPHR Measuring Cyberabuse Survey, a nationally representative telephone survey conducted on cell phones and landlines, interviewing 3,002 American internet users ages 15 and older. The survey was conducted by Princeton Survey Research Associates International (PSRAI) and funded by the Digital Trust Foundation. Survey design and data analysis were executed by staff at the Data & Society Research Institute and the Center for Innovative Public Health Research. Interviews were administered in English and Spanish by Princeton Data Source from May 17 to July 31, 2016. Statistical results are weighted to correct known demographic discrepancies. The margin of sampling error for the complete set of weighted data is ±2.0 percentage points. For more detail, please see the Methods page at http://datasociety.net/pubs/oh/methods.pdf

.

Data & Society is a research institute in New York City that is focused on social, cultural, and ethical issues arising from data-centric technological development. To provide frameworks that can help address emergent tensions, D&S is committed to identifying issues at the intersection of technology and society, providing research that can ground public debates, and building a network of researchers and practitioners that can offer insight and direction. To advance public understanding of the issues, D&S brings together diverse constituencies, hosts events, does directed research, creates policy frameworks, and builds demonstration projects that grapple with the challenges and opportunities of a data-saturated world.

The Center for Innovative Public Health Research, also known as CiPHR, examines the impact that technology has on health and how it can be used to affect health. We have developed programs to reduce HIV transmission, increase smoking cessation, and provide supportive resources for youth experiencing cyberbullying and people with depression. CiPHR is a non-profit, public health research incubator founded under the previous name, Internet Solutions for Kids, Inc. (ISK). Our vision is to promote positive human development through the creation and implementation of innovative and unique technology-based research and health education programs. Public health is ever evolving and so are we.

Contact

Amanda Lenhart
amanda@datasociety.net
Data & Society Research Institute
36 West 20th Street, 11th Floor New York, NY 10011
Tel. 646-832-2038
datasociety.net

Notes

Keywords: Revenge porn, nonconsensual image sharing, nonconsensual pornography, nude images, nude video, sexually explicit material, online harassment, online abuse, digital domestic abuse

Data & Society Research Institute
CiPHR Center for Innovative Public Health Research

Data & Society Research Institute
36 West 20th Street, 11th Floor
New York, NY 10011
Tel 646.832.2038
Fax 646.832.2048
info@datasociety.net