



NATIONAL NETWORK
TO END DOMESTIC
VIOLENCE

1400 16TH STREET NW
SUITE 330
WASHINGTON, DC 20036

www.nnedv.org
phone: 202.543.5566
fax: 202.543.5626

March 2, 2015

Via Electronic Submission

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex D)

Re: Craig Brittain—Consent Agreement: File No. 1323120

Dear Commissioners:

The National Network to End Domestic Violence (NNEDV) believes that the Consent Agreement File No. 132 3120 is an important first step in addressing devastating harm to consumers, particularly victims of abuse, stalking, and violence. NNEDV is a social change organization dedicated to creating a social, political, and economic environment in which violence against women no longer exists. Founded in 1990, NNEDV represents 56 state and territory domestic violence coalitions, who in turn represent nearly 2,000 local domestic violence service providers across the country.

The issue of non-consensual sharing of sensitive images is very important to the Safety Net Technology Project at NNEDV. NNEDV's Safety Net Project addresses how technology impacts safety, privacy, accessibility, and the civil rights of victims. Safety Net works with communities, victim service agencies, and technology companies to:

- Address how technology impacts survivors of abuse and stalking;
- Educate victim advocates and other professionals on how to use technology strategically to increase safety;

- Train criminal justice professionals on tactics of technology misuse in the context of domestic violence, sexual assault, dating abuse, trafficking, and stalking;
- Advise technologists on technology risks and benefits to victims; and
- Advocate for strong policies that ensure the safety and privacy of victims.

Since 2002, the Safety Net team has presented nearly 1,000 trainings to more than 71,000 people and responded to more than 13,500 unique requests for assistance and resources. Through in-depth consultations, the Project helps service providers on a range of issues, including complex technology-facilitated abuse and stalking cases, implementing technologies such as developing secure online chat systems, and developing best practices on how to use new technologies safely. The Safety Net Team also works closely with technology companies such as Verizon, Google, and Facebook and serves on Facebook's Safety Advisory Board.

The Safety Net Project recently surveyed victim service providers on the misuse of technology by abusers. Of the programs surveyed, 97 percent reported that the survivors they work with experience harassment, monitoring, and threats by abusers through the misuse of technology.¹ The survey also found that 55% of programs reported that victims they work with had abusers who posted intimate photos of them online without consent.



Images of victims are often distributed online as a tactic of abuse by perpetrators who want to harass, humiliate, or cause harm to the victims. Abusers often include personal information about the victims, including their home or work addresses and phone numbers. These images are often distributed without consent and are sometimes obtained through means of extortion, blackmail, and even hacking. Websites that post these images not only profit from these images (one site saw 30 million pageviews and earned \$13,000 a month before it was shut down²), they further extort victims by making them pay fees to remove the photos from the site.

¹ http://techsafety.org/s/NNEDV_Glimpse-From-the-Field-2014.pdf

² <http://www.theawl.com/2011/11/the-man-who-makes-money-publishing-your-nude-pics>



When sensitive and intimate images of victims, along with personally identifying information, are shared without their consent, victims are at significant risk for further abuse, stalking, and harassment. After their picture or video and personal information have been posted online, victims have been harassed by strangers who demand sexual acts or coerce victims into meeting them. Victims are blackmailed for more sexually explicit images or financially exploited with promises of returning the images back to the survivor or removing the pictures from distribution.

Mr. Brittain deceived women into sharing nude photos with him and posted them on his website without consent, paid others to share nude photos, and published victims' personally identifying information along with the photos. He extorted victims by making them to pay to have their pictures removed (and did not always remove the photos, even after receiving payment)³. His actions not only harmed these women by posting their private, intimate images publicly; he put them at risk for further victimization, including stalking, harassment, and assault.

Despite the high prevalence of this type of abuse (and approximately 3,000 websites featuring 'revenge porn' in existence⁴), only sixteen states have laws that explicitly criminalize the non-consensual publication of intimate photographs⁵. Moreover, as these images go "viral," so does the abuse. Abusers are able to "crowd-source" their harassment, while unscrupulous individuals profit from it, and victims often have very little recourse.

Although significantly more needs to be done to hold abusers and those who profit from these reprehensible acts accountable, and penalties need to be more substantive to deter those who seek to harm victims, the proposed consent agreement in the Matter of Craig Brittain is an important first step in holding at least

³ <http://www.ftc.gov/system/files/documents/cases/150129craigbrittainanalysis.pdf>

⁴ The Economist, Revenge Porn: Misery Merchants, July 5, 2014.

⁵ Alaska, Arizona, California, Colorado, Delaware, Georgia, Hawaii, Idaho, Illinois, Maryland, New Jersey, Pennsylvania, Texas, Utah, Virginia, and Wisconsin.

one operator of these heinous websites accountable for his actions.

Respectfully submitted,

Cindy Southworth, Executive Vice President and founder of the
Safety Net Project at NNEDV
Kristelyn Berry, Safety Net Project Coordinator
Rachel Gibson, Technology Safety Specialist
Kaofeng Lee, Deputy Director of the Safety Net Project
Leslie Malkin, Technology Safety Specialist
Erica Olsen, Deputy Director of the Safety Net Project