# When A Leader **Becomes the Victim**

Tamarin Lindenberg, Managing Partner

Lindenberg Law Group

Indianapolis, October 5-7, 2023

NAWJ

45th ANNUAL CONFERENCE

SETTING THE PACE FOR JUSTICE

# Cyber Violence Against Professional Women

| | | |
|---|---|---|
| Interviews with a wide range of leaders and constituents | → | No one likes to talk about it |
| Professional women do not want the stigma of victim | → | Try to self-manage the damage |
| Law enforcement | → | Threats not taken seriously<br>Some frustration and concern |

# Dangerous Reality

**41%*** of adults experience online harassment

**25%** experience physical threats, sexual harassment and harassment over an extended period

**28%** experience multiple forms of harassment

**Women make up the majority harassed and threatened online**

**No data yet to distinguish harassment of women based on their professional role but some studies shows that over 70% is the result of their political affiliation**

* Credit: 2020 Pew Research Study

# Responses of Investigators

“Women shouldn’t be working in the first place. They take jobs away from men.”

Harassment an “annoyance” and downplayed actual risk of escalation

Little concern for women who “make more than they do”

Cases “too hard to prove”

Women “have a place” —not in positions of authority over men

# Forced to Choose

- Overwhelming theme was **lack of resources**
- **Limited personnel** to track cyber-violence
- **Restrictions** in government agencies
- Need for NGOs **focused on non-domestic cyber-violence**
- **Efforts are siloed** without a strong base for sharing information

# Heroic Responses from Law Enforcement

### FRUSTRATION

towards colleagues who did not properly distinguish victimology in online stalking and harassment

### ACKNOWLEDGMENT

of cyber-violence against women in leadership as differing greatly from domestic violence and revenge porn

### DETERMINATION

to support our efforts to protect women in leadership roles

### CONCERN

for their wives and daughters in professional settings

### DISSATISFACTION

over the inability to hold perpetrators accountable—most referred to Section 230 of the Communications Act which gives tech companies immunity for harassment campaigns on their sites

# Emotional Response Cycle of Victims

**DENIAL:** The hope that ignoring it will “make it go away”

**SHAME AND EMBARASSMENT:** Exacerbated by the deflection of those in charge

**ISOLATION:** Attempt to hide attacks–fear of loss of reputation; feeling of abandonment

**SENSE OF WORTHLESSNESS:** Lingering question–why the victim isn’t valued enough to protect

**DISASSOCIATION:** An effort to compartmentalize harm to enable the victims to carry out ongoing responsibilities

**PROBLEM SOLVING:** Progression into action for large scale solutions; become advocates and changemakers

# Reactions of Female Leaders Who Sought Help

- Demand for distinction between revenge porn and harassment due to leadership role
- Anger at the lack of effort offered by law enforcement
- Cited the stress of attack worsened by attitudes of law enforcement
- Difficulty in finding legal assistance educated in the topic
- Frustration with lack of knowledge of the topic in the legal community
- Loss of income and reputational damage
- Fear for safety of family

# This is **Not** Revenge Porn

Incredible work has been done to protect women from revenge porn. The term has become synonymous with online abuse of women **BUT it's not the whole story**

Women in leadership roles are under **increasing attacks involving sexual exploitation** where **no personal relationship exists**

These attacks are **about power and control and use humiliation and intimidation** to diminish professional standing

# A Definition


Women in key roles of influence


Sexual exploitation unrelated to domestic violence and revenge porn

Used as a growing method for silencing women


# Risk of Escalation

- Affecting those in business, law, politics, media, and virtually **every other area where women exhibit leadership and influence**
- **Threatens** income earning opportunities, destroys professional relationships and breaches security.
- Where an online presence is paramount to business development victims are doubly challenged with **little recourse for protection.**
- Attacks can and do devolve into **threats against physical safety.**

# Members of the Judicial Community Face Exposure to Acts of Retaliation

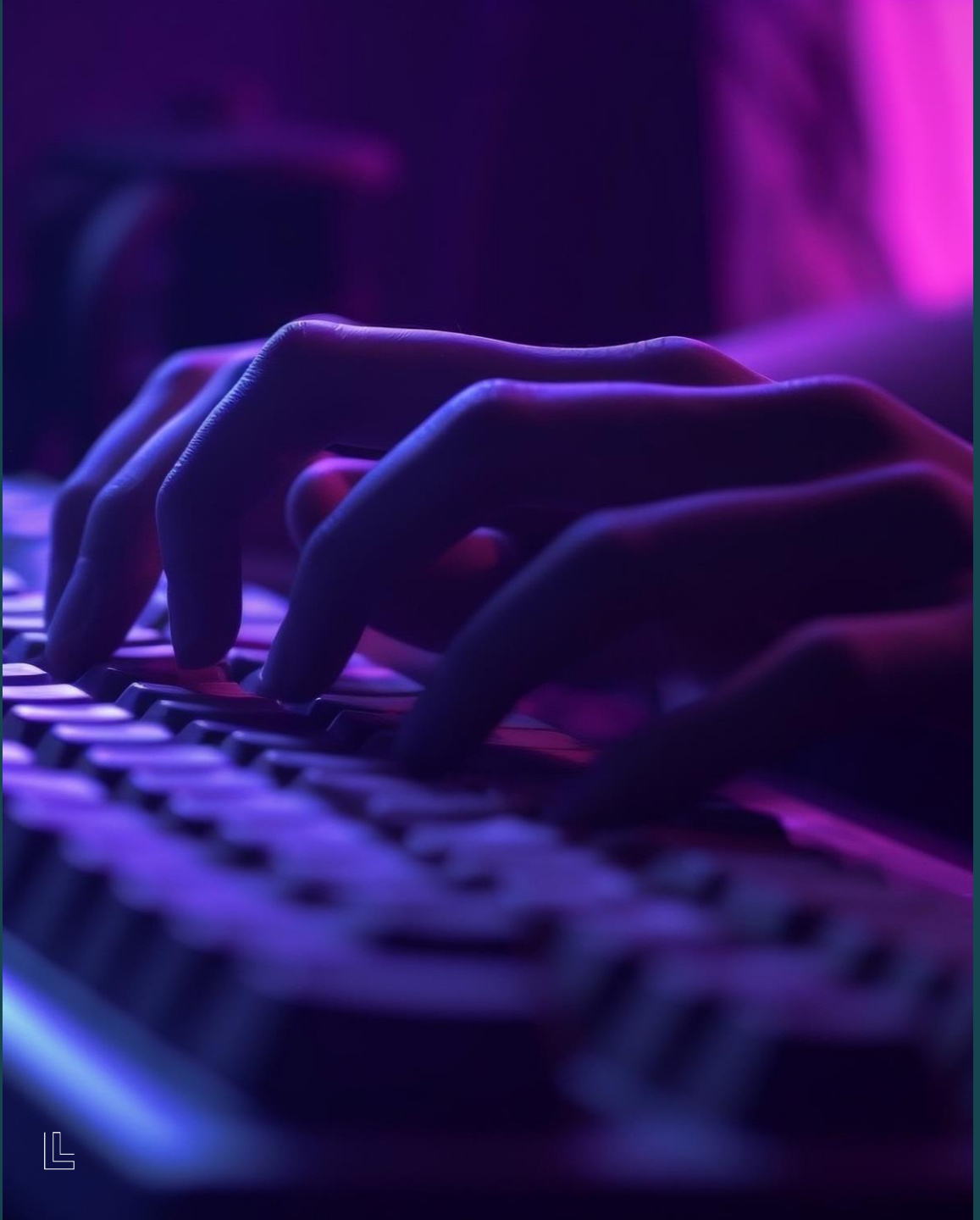
- In 2020, Judge Salas suffered irreparable loss at the hands of a Manhattan lawyer and self-described anti-feminist who stalked her online and gained her personal information. The result was unthinkable.
- When Judge Robart issued a temporary restraining order on President Trump's first travel ban, he received over 1,100 serious threats. His personal information was put online, along with his wife's information—a threat to her safety.
- U.S. Marshals Service tasked with protecting federal judges reported 4,449 threats and inappropriate communications against protected persons in 2019.
  In 2015, that number was 926.
- Inappropriate communications or threats to protected court family members have also been on the rise. There were 4,542 reports of threats or inappropriate communications to family members in 2018. In 2014, that number was 768.

The New York Times

# NY Times Reported September 2023

- Threats against law enforcement, judges and elected officials are on the rise.
- FBI agents have raised alarms about harassment and threats targeting their families.
- Law enforcement and our judicial system are viewed as the enemy.
- The FBI has witnessed a substantial surge in threats against its personnel and facilities since August 2022.
- This led the agency to establish a dedicated unit to address these threats.
- One federal official told the Times that threats have increased by more than 300% since 2022, partly because FBI agents' identities and personal information has been spread on social media.

# Tools of the Dark Web



# Spoofing

Abusers pretend to be someone else so victim picks up the phone

They impersonate the victim as they call others, entering the victim’s phone number as the “caller”

Record conversations/video of the victim to get more information—keep power and control over the victim

Change caller ID numbers and alter voices so their call appears to come from another gender or another person

# Electronic Surveillance

Abusers monitor actions or conversations without knowledge or consent, using one or more electronic devices or platforms.

An abuser may use recording and surveillance technology to “keep tabs” on the victim by monitoring whereabouts and conversations.

Their motive—to maintain power and control, make it hard for the victim to have a life separate from the abuser’s fantasy, and/or to try to reveal plans made to stop the abuser.

Abusers misuse monitoring software (also known as spyware), which can be installed on a computer, tablet, or a smartphone to secretly monitor the device activity

Spyware can allow the abusive person access to everything on the phone, as well as the ability to intercept and listen in on phone calls.

# Cyber-Surveillance

Use of “smart” or “connected” devices—monitor/communicate via a data network

TV 's are often connected to the Internet controlled with an app on your phone

These devices and systems increase our safety and convenience

Also allow connected devices to play a role in how people and places are monitored by abusers

Abusers uses computer (or other devices  connected to the Internet—phone or tablet) to hack into victim’s devices

Misuse these devices and the systems to monitor, harass, threaten, or harm the victim

# GPS Tracking

Location information through the GPS in your phone is not automatically available to another person, but there are a variety of ways that an abuser can get it:

- share a cell phone plan (common among business plans)
- spyware, downloaded apps, or accessed when devices are synced to the “cloud” or computer

**Abusers use this technology to stalk or to maintain power and control over a victim**

# Impersonation

## SOCIAL MEDIA

Abusers create fake accounts in the victim's name, hack into their legitimate accounts, or manipulate technology in a way that makes it seem like a communication is coming from the victim.

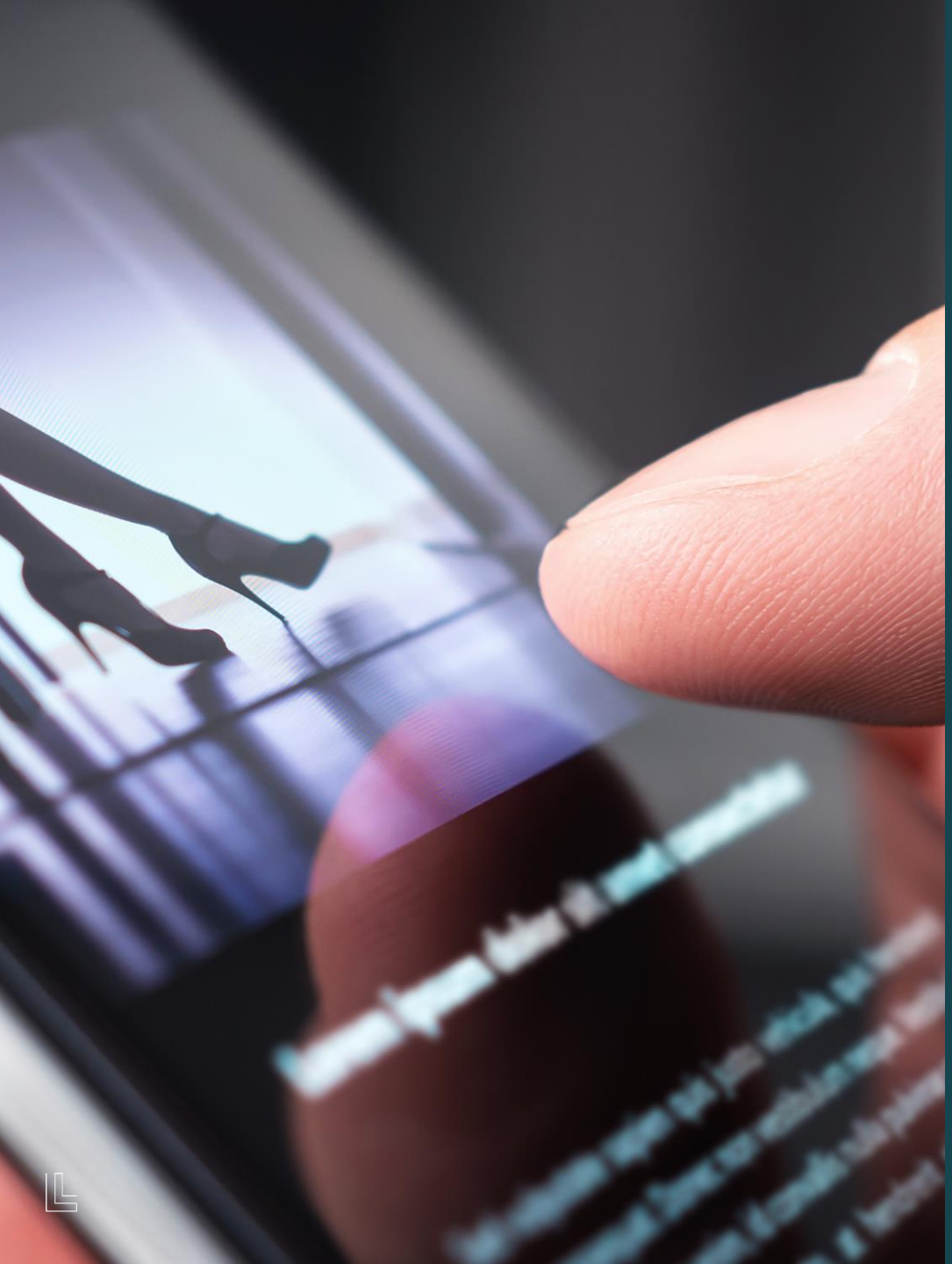
Abusers use fake accounts impersonating the victim to post fake messages to cause public backlash

They impersonate the victim to get information about the victim.

## EMAIL

Create fake email accounts to send harassing emails while masking their identity as the sender.

Create an email account in the victim's name, sending emails to others to embarrass, discredit, put at risk of harm, or cause some other negative consequences in the victim's life.



# Online sexual impersonation

Abusers use the victim's private information to pose on the Internet and invite others to harass their target or put them in danger.

An abuser may create an advertisement (posing as the target) directing others to contact the victim for escort or sexual services, or invite others to come to the target's home for a harmful purpose.

Abusers use impersonation to encourage others to sexually assault their target.

An abuser may include information in the advertisement or online post that states the target has a "fetish" or "fantasy". The purpose of these types of online posts is to cause a third party to carry out an assault

# Deep Fake

## Deep fake is rapidly maturing in its ability to create visual and audio depictions

Sensity AI has tracked online deep fake videos since 2018 – **90%-95% are nonconsensual porn.**

Images are lifted off social media platforms and apps such as **deepnude** and coded to “strip” clothes from victims.

Though these apps were banned, the underlying code remains available.

The images often call upon viewers to act out violence, abuse and humiliation upon the victim. They often depict the victim in degrading and tortuous acts to stimulate the audience.

46 states have some ban on revenge porn but only CA and VA include fake and deep fake media.

Photo: thestar.co.uk

Helen Mort, a broadcaster, was a deep fake victim after a perpetrator uploaded holiday and pregnancy photos from her private social media accounts. These photos were altered to create nude photos for porn sites in a harassment campaign to silence her.

Helen contacted police who said they could do nothing which is a common response. She tried to end her online presence but needed to have one for her business. She fought back in efforts to raise awareness.

# Who are the Abusers and Third Parties?

**Public Corporations**

**Private Businesses**

**Lawyers**
Yes, as stalkers. Yes, as third parties.

**Public Figures**

**Business Competitors**

**Ex-employees**

**Law enforcement**
Yes, as stalkers. Yes, as third parties.

**Political leaders**

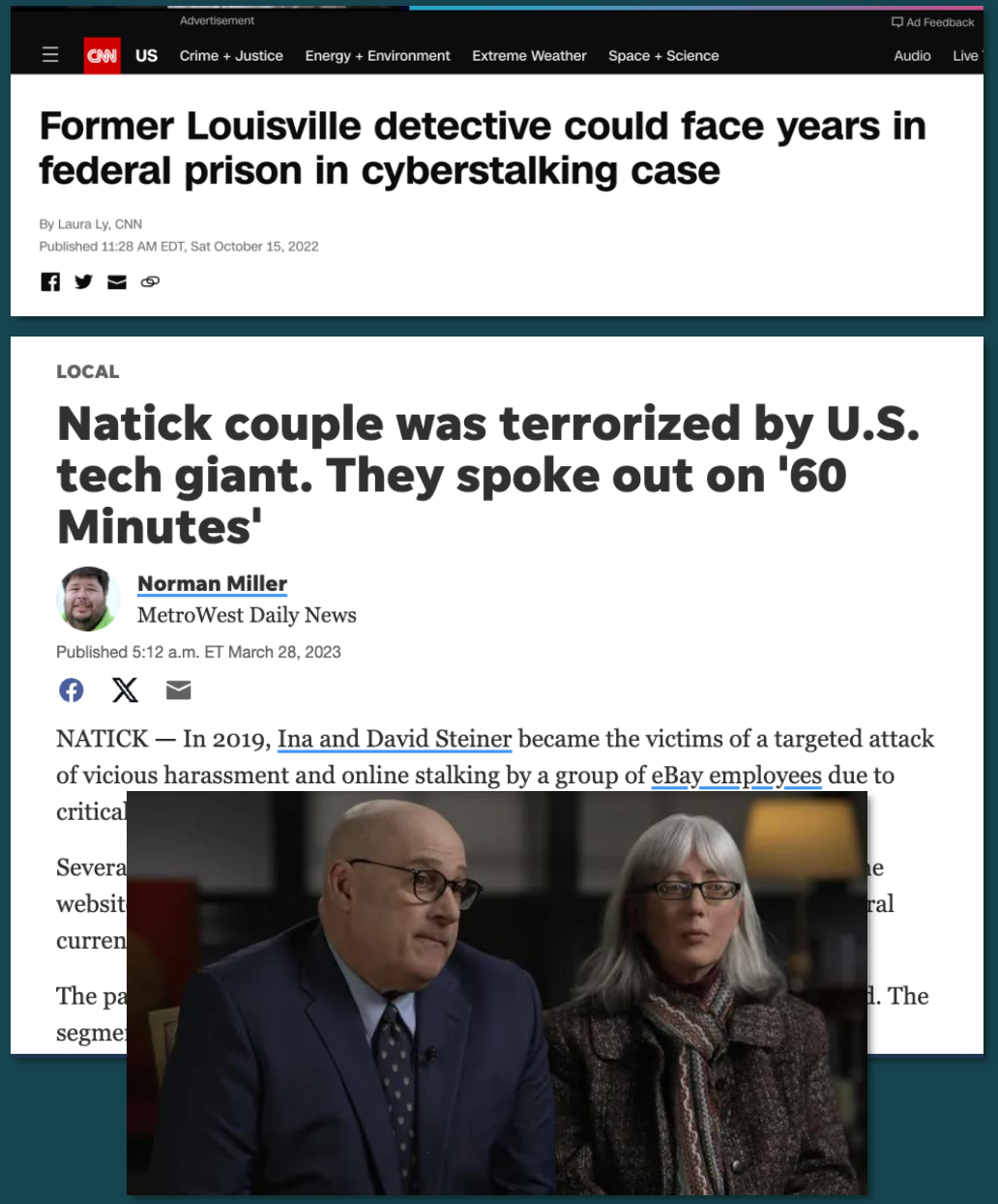
# The Unexpected

**Louisville detective** convicted of cyber-stalking women used law enforcement access to gain information about female victims who had reported being hacked.

7 **eBay employees** pled guilty to criminal conspiracies after engaging in the aggressive harassment of 2 ecommerce bloggers. Two of the stalkers were senior members of the eBay security team. 2 members of the exec leadership team were implicated but not charged

**Visa** named as third-party defendant in a case involving sexual exploitation

**JP Morgan** paid $290M settlement to Epstein victims



Advertisement

Ad Feedback

CNN US Crime + Justice Energy + Environment Extreme Weather Space + Science Audio Live

**Former Louisville detective could face years in federal prison in cyberstalking case**

By Laura Ly, CNN
Published 11:28 AM EDT, Sat October 15, 2022

LOCAL

**Natick couple was terrorized by U.S. tech giant. They spoke out on '60 Minutes'**

Norman Miller
MetroWest Daily News

Published 5:12 a.m. ET March 28, 2023

NATICK — In 2019, Ina and David Steiner became the victims of a targeted attack of vicious harassment and online stalking by a group of eBay employees due to critical

Severa … websit … curren …

The pa … segme … d. The

# Who We Are

We are an **ABS law firm licensed under the Utah Office of Innovation and Utah Supreme court**

---

We are a **non-attorney owned law firm** with a multidisciplinary team

---

We are the **first law firm to study the impact issues** of cyber-violence against women in leadership and the **first to create a multidisciplinary approach** to drive relief for victims

---

We believe the challenges to access to justice are **not limited to the indignant but include those whose matters involve emerging areas of law**

# What We Have Done

Our work has **redefined victims and abusers outside of domestic violence.** This is key to bringing **proper relief.** We have investigated this form of cyber-violence from multiple angles **for the last 4 years.**

# What We Have Done

**We have** identified the biases as well as the emotional and tactical responses of each role

**We have** identified root issues that connect cyber-violence against multiple target groups and are building inroads to share information to stop abusers.

**We have** dedicated countless hours to exploring powerful causes of action for these cases

**We have** evaluated initial social responses, delivered educational opportunities and re-evaluated responses to measure new learning

**We have** called out gaps in the legal industry and created ways to  be part of the solution

**We have** embraced and explored emerging technology and the critical role it can play in complex cases

# How Have We Used the Insights Gained?

1

## IDENTIFIED

underutilized statutes; ie, violation of constitutional rights, business interference, RICO, hate crimes, terrorism

2

## ANALYZED

damages from unique perspectives that measure the impact of ongoing trauma vs a singular event

3

## ESTABLISHED

a robust team with deep expertise in cyber-violence for more holistic solutions in emerging areas of law

4

## DEVELOPED

tools to educate the legal profession on this emerging area & instituted opportunities for collaboration

# What Are We Planning Next?

1

## PURSUING

cases that set precedent and properly award victims

2

## EXPLORING

opportunities to align with like-minded talent

3

## RAISING

support for advances in awareness and legislation

4

## LAUNCHING

summit in DC to bring policymakers together with those most impacted

# Your Safety

Know the tools that can be used against you in your roles as leaders

Support those under attack and openly seek support if you are victimized

Realize that families are a second level of attack and guard accordingly

Engage in the conversation and remove the stigma for plaintiffs

Join us in increasing accountability for those who harm

# High Impact Considerations

Recognize these cases are not revenge porn or domestic violence

Understand the use of cyber-violence as a tool for economic, emotional and reputational harm to those in leadership roles

Know that cyber-violence often escalates to physical violence

Know that victims most often experience extraordinary and ongoing stress greatly reducing quality of life

Recognize the abusers in these cases are competitors, business associates, lawyers, ex-employees, and others connected through professional relationships

Engage Neutrals with **DIRECT SUBJECT MATTER EXPERTISE** to support court cases and mediation efforts

It makes you feel powerless, like you're being put in your place. Punished for being a woman with a public voice of any kind. It's saying **"look, we can always do this to you."**

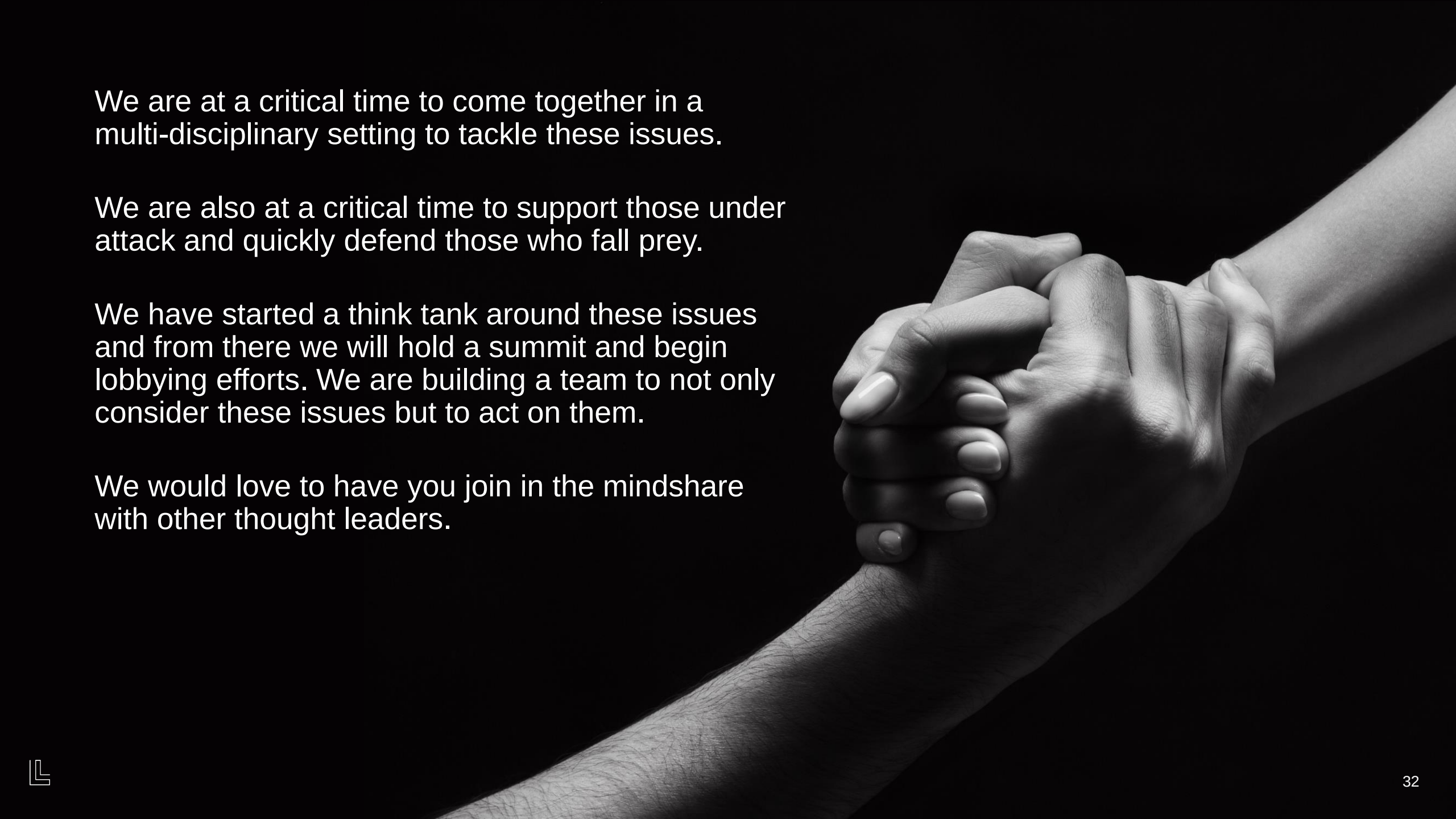
Helen Mort

We are at a critical time to come together in a multi-disciplinary setting to tackle these issues.

We are also at a critical time to support those under attack and quickly defend those who fall prey.

We have started a think tank around these issues and from there we will hold a summit and begin lobbying efforts. We are building a team to not only consider these issues but to act on them.

We would love to have you join in the mindshare with other thought leaders.



# Our Team

**Tamarin Lindenberg**
Founder

**T. Keith Fogg, Esq**
Professor of Law, Emeritus, Harvard/Retired IRS Counsel

**Amanda Moore**
Public Relations / Producer

**Zach Lindenberg**
Operations

**Jeremy Babener, Esq**
Tax Strategist

**Joe Di Gangi**
Settlement Architect

**Todd Yurasek**
IT Director

**Edward W. Reinhold**
Retired FBI/COO
NCOSE

**Joseph Scaramucci**
Lead Investigator

**Jeni Stewart**
Creative Director

Lindenberg Law Group

**Tamarin Lindenberg, Managing Partner**

**Phone: 901.230.3890 | email:** tamarin@lindenberglawgroup.com