

10 TIPS TO PROTECT AGAINST DEEPPFAKE EVIDENCE

“Your digital self is
evidence. Protect it like
your **future** depends on it
— because it does.”



Michelle O'Neil
Legal Strategist
@TheMichelleOneil





@TheMichelleOneil

PROTECT YOUR DIGITAL FOOTPRINT

- Lock down social media accounts: set profiles to private, limit who can see or download your photos and videos.
- Remove old, unused accounts that may still contain media someone could scrape and misuse.
- Be extremely cautious about what new photos, videos, or even comments you share publicly during your case.

Michelle O'Neil
Legal Strategist
@TheMichelleOneil

@TheMichelleOneil

SAVE ORIGINAL CONTENT

- Keep original versions of your photos, videos, emails, and texts.
- Having metadata (timestamps, location stamps) can help prove what's authentic if false content surfaces.

Michelle O'Neil
Legal Strategist
@TheMichelleOneil





@TheMichelleOneil

MONITOR YOUR ONLINE PRESENCE

- Set up Google Alerts on your name and any known variations (including nicknames).
- Regularly search your name + keywords like “video,” “photo,” or “scandal” to detect anything suspicious early.

Michelle O’Neil
Legal Strategist
@TheMichelleOneil

@TheMichelleOneil

CHALLENGE AUTHENTICITY IMMEDIATELY

- If you are confronted with suspicious evidence in court (texts, videos, photos), do not concede that it's real without independent verification.
- Request formal authentication (forensic analysis) before responding substantively.

Michelle O'Neil
Legal Strategist
@TheMichelleOneil





@TheMichelleOneil

DEMAND METADATA IN DISCOVERY

- In litigation, always request the original digital files plus metadata — not just screenshots or clips.
- Fake evidence often breaks down under metadata analysis because synthetic files are missing key creation details.

Michelle O'Neil
Legal Strategist
@TheMichelleOneil

@TheMichelleOneil

INVOLVE A DIGITAL FORENSICS EXPERT

- If deepfake or manipulated evidence is suspected, involve a certified forensic expert early.
- They can analyze telltale signs like frame anomalies, audio mismatches, lighting inconsistencies, and metadata tampering.

Michelle O'Neil
Legal Strategist
@TheMichelleOneil



@TheMichelleOneil

EDUCATE YOUR ATTORNEY

- Not all attorneys are familiar with deepfake technology.
- If needed, suggest involving experts or cite the risks — you are your own best advocate.

Michelle O'Neil
Legal Strategist
@TheMichelleOneil

@TheMichelleOneil

SEEK **EMERGENCY** **RELIEF IF** NECESSARY

- If synthetic media is circulated or threatened, file immediately for emergency injunctions or protective orders.
- Cite the TAKE IT DOWN Act if non-consensual intimate imagery is involved.

Michelle O'Neil
Legal Strategist
@TheMichelleOneil





@TheMichelleOneil

PRESERVE ALL EVIDENCE

- Screenshot threats or suspicious activity.
- Save full URLs, messages, profiles, or postings. Preservation can make or break your case if removal occurs later.

Michelle O'Neil
Legal Strategist
@TheMichelleOneil

@TheMichelleOneil

STAY CALM AND STRATEGIC

- Accusations around synthetic media can cause panic — which can be weaponized against you.
- Stay composed, gather your proof, and work methodically through legal channels.

Michelle O'Neil
Legal Strategist
@TheMichelleOneil





@TheMichelleOneil

“Your digital self is **evidence**. Protect it like your **future** depends on it — because it does.”

Michelle O’Neil
Legal Strategist
@TheMichelleOneil