



Open SSL Conference

What you ship might sue you

Presented by Ashley Pusey, CIPP/E/US, CIP,
FIP

October 2025

Kennedys

DISCLAIMER

This presentation and its contents are provided 'AS IS', without warranties or conditions of any kind.

- No guarantee as to accuracy, completeness, or applicability
- Nothing herein constitutes legal advice
- All examples are illustrative only
- By relying on this material, you assume all risks

Changing Tides

Adopting to New Currents in Law and Technology

- EU AI Act – liability for high-risk AI, documentation + accountability duties
- US Government – AI Action Plan has a deregulation and pro-innovation agenda
- States – liability for high-risk AI, shifting legal theories and risks to developers
 - Ex: Rhode Island S0358 (died in committee March 18, 2025)
- Court Shift of Product Liability Reform – software may be treated like a “product”
 - Ex: Garcia v. Character Technologies, Inc. 6:24-cv-01903, (M.D. Fla. Oct 22, 2024)
- Developers = increasingly named in legal debates.



Rising Waters – The New Waive of Liability

Legal risk and emerging liability theories

- Negligence – did the developer meet a “reasonable standard of care”?
- Product liability – defective software = defective product.
- Failure to warn – inadequate documentation/disclaimers.
- IP infringement – training copyrighted data on LLMs mixing patented code.
- Regulatory breach – non-compliance with legal frameworks.
- “Upstream Liability” – Developers upstream → users downstream drinking the water. If toxins (bad practices) are dumped upstream, the regulators/law may hold the *source* accountable.

Storm Warnings

All Hands-on Deck – Who Bears the Risk?

AI LEAD Act - introduced in the Senate Sept. 29, 2025

Developer requirements at the state level / other global regulations (e.g. EU AI ACT)

Garcia v. Character Technologies, Inc. - 6:24-cv-01903, (M.D. Fla. Oct. 22, 2024)

Raine v. Open AI, et al (Aug. 26, 2025)

Case study - Garcia v. Character Technologies, Inc.

6:24-cv-01903, (M.D. Fla. Oct 22, 2024)

- Lawsuit filed after a 14-year-old committed suicide following interactions with Character A.I. chatbots
- Plaintiff asserted strict liability design defect → chatbot is a defectively designed “product”
- May 21, 2025 → Court allowed the claim to proceed → treating AI app as a “product” under strict liability law



Gray Areas – Uncharted Territory

Open source isn't on Trial – it's *how* it is used and the *functionalities* of the product

Where maintainers *potentially* get pulled in the cross hairs

- When a company funds or “employs” maintainers (e.g., corporate open-source teams), courts could see that as commercial distribution.
- If maintainers actively represent safety or compliance claims (“secure-by-design,” “AI-safe”), they might create express warranties.
- If they know of a critical flaw and continue to promote the code for sensitive use, negligence theories could surface (esp. under expanded “duty of care” language in LEAD-style bills).

Open Source → Implementer/Developer → Product → User → Harm
(open source) (liability threshold) (exposure)

Who's in the crosshairs (potentially)

How Liability Pulls in Developers



Developers who integrate or ship code to a product.



Maintainers who actively represent safety or compliance claims may create express warranties (“AI-safe” or “Secure-by-design”)



Infrastructure builders secure-by-design expectations, “knew or should have known” standard.

Rethinking “incident response”

Beyond Security → Incident Response for Code & AI

Classic IR Plan (Cybersecurity)



Data breach notifications



Forensics & log analysis



Regulator engagement

PR/
communications

Developer IR Plan (Alternative Lens)



User Notification

Rapidly inform downstream users when code is flawed or dangerous



Mitigation Guidance

Provide practical “what to do now” steps for users



Kill Switch / Rollback

Ability to disable, revert, or patch quickly




Transparency Logs

Public changelogs or advisories document fixes



Human Harm Scenarios


Special protocols if AI output causes risk (suicidal ideation).

✓ Licensing Hygiene 

✓ Disclaimer Hygiene 

✓ Contribution Hygiene 

✓ Security Hygiene
→ Legal Hygiene Tie-In 

✓ Incident Hygiene 

✓ Shield Hygiene 

**Developer legal
hygiene checklist
considerations**

Closing remarks



Courts are experimenting, and liability theories are evolving.



Whether you're building an AI chatbot, shipping an update, or maintaining open-source code — the choices you make matter.”



You can't code away liability, but you can *code with it in mind*.



Think about *legal hygiene* the way you think about *security hygiene*.

Let's connect!



Ashley Pusey

Associate
New York

+1.646.625.3998


ashley.pusey@kennedyslaw.com


Ashley Pusey, CIPP/US/EU, CIPM, FIP
Privacy, AI & Cyber Attorney
| Translating Complex Tech & Pri...



Kennedys

 Kennedys

 KennedysLaw

 KennedysLaw

 KennedysLaw

Kennedys is a global law firm operating as a group of entities owned, controlled or operated by way of joint venture with Kennedys Law LLP.
For more information about Kennedys' global legal business please see kennedyslaw.com/regulatory

kennedyslaw.com