Oregon State Bar CLE Seminars

# Cracks in the Foundation: Problems with Internet and Tech Companies

*Cosponsored by the Technology Law Section*

Thursday, November 10, 2022
9 a.m.–12:15 p.m.

3 Access to Justice credits (ID 94410)

## SECTION PLANNERS

**Aaron Cronan,** *Cronan Law LLC, Portland*
**Shiwanni Johnson,** *Crew Janci LLP, Portland*

## OREGON STATE BAR TECHNOLOGY LAW SECTION EXECUTIVE COMMITTEE





OREGON STATE BAR
16037 SW Upper Boones Ferry Road
P.O. Box 231935
Tigard, OR 97281-1935

## TABLE OF CONTENTS

## SCHEDULE

**9:00 The True Predators: Big Tech's Role in Child Exploitation**

- ✦ Case studies in online predation of kids
- ✦ Access to justice issues for victims of sextortion, including Section 230
- ✦ Progress in holding platforms liable, including a look at A.M. v. Omegle (Oregon District Court)
- ✦ What's next regarding regulation of tech companies

Carrie Goldberg, *C.A. Goldberg PLCC, Brooklyn, New York*
Barbara Long, *Vogt & Long PC, Portland*

**10:30 Break**

**10:45 Challenges to Building Trust in Artificial Intelligence/Machine Learning: An Exploration of Data Bias, Model Bias, and Explainability**

- ✦ Socio-technical systems like AI, algorithmic, and autonomous systems are increasingly being used by enterprises in the US and globally
- ✦ Basics about machine learning model operationalization management (MLOps) lifecycles and where bias is lurking
- ✦ Emerging tools for detection and mitigation
- ✦ Evolving US/EU regulation for accountability, governance, and oversight

Caryn Lusinchi, *BiasInAI.com, Portland*

**12:15 Adjourn**

## FACULTY

**Carrie Goldberg,** *C.A. Goldberg PLCC, Brooklyn, New York.* Ms. Goldberg is a victims' rights attorney. She is a member of the Cyber Civil Rights Initiative board, the Lawyers Committee Against Domestic Violence Family Court Working Group, the [New York] City Bar Committee on Domestic Violence, and the New York State Bar Association Committee of Women in the Law Legislative Subcommittee. She also is a founding member of the New York City Cyber Sexual Exploitation Task Force and was a member of California Attorney General Kamala Harris's Cyber Exploitation Working Group Law Enforcement Subcommittee. She is admitted to practice in New York and before the United States Supreme Court. She is the recipient of the 2020 Domestic Violence Legal Empowerment and Appeals Project Joan Meier Founder's Award for her work transforming the legal landscape for domestic violence survivors. She also received the 2017 Privacy Champion Award from Electronic Privacy Information Center. Ms. Goldberg is the author of *Nobody's Victim* (Plume, 2019).

**Barbara Long,** *Vogt & Long PC, Portland.* Ms. Long almost exclusively represents survivors of sexual abuse and exploitation. She is active in the Oregon Trial Lawyers Association, where she cochairs the Women's Caucus and Publications Committee. She also serves on the Oregon State Bar House of Delegates. Ms. Long regularly writes and speaks on topics related to her practice.

**Caryn Lusinchi,** *BiasInAI.com, Portland.* Ms. Lusinchi provides consultation and strategy services for leading global companies, business decision-makers, and investors. Ms. Lusinchi works for Arthur, a Series B software company monitoring data accuracy, bias, fairness, and explainability for machine learning models in production, and for Andromeda AI, the parent company of Bias in AI. She also works with AI chat bots, voice virtual assistants, and conversational design; content design and optimization; RFP authoring and scoping; accessibility, data privacy, and compliance; and management training. She is a ForHumanity Certified Auditor (FHCA) under UK, EU GDPR, and NYC Bias Law and holds a certificate in Foundations of Independent Audit of AI Systems (IAAIS).

# Chapter 1

# The True Predators: Big Tech's Role in Child Exploitation

**Carrie Goldberg**
C.A. Goldberg PLCC
Brooklyn, New York

**Barbara Long**
Vogt & Long PC
Portland, Oregon

**Contents**

# 47 USCS § 230

Current through Public Law 117-185, approved October 4, 2022.

***United States Code Service > TITLE 47. TELECOMMUNICATIONS (Chs. 1 — 16) > CHAPTER 5. WIRE OR RADIO COMMUNICATION (§§ 151 — 646) > COMMON CARRIERS (§§ 201 — 276) > COMMON CARRIER REGULATION (§§ 201 — 231)***

## § 230. Protection for private blocking and screening of offensive material

**(a) Findings.** The Congress finds the following:

**(1)** The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

**(2)** These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

**(3)** The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

**(4)** The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

**(5)** Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

**(b) Policy.** It is the policy of the United States—

**(1)** to promote the continued development of the Internet and other interactive computer services and other interactive media;

**(2)** to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

**(3)** to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

**(4)** to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

**(5)** to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

**(c) Protection for "Good Samaritan" blocking and screening of offensive material.**

**(1)** Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

**(2)** Civil liability. No provider or user of an interactive computer service shall be held liable on account of—

**(A)** any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

**(B)** any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1) [subparagraph (A)].

**(d) Obligations of interactive computer service.** A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

**(e) Effect on other laws.**

**(1)** No effect on criminal law. Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this Act [*47 USCS § 223* or *231*], chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code [*18 USCS §§ 1460* et seq. or *§§ 2251* et seq.], or any other Federal criminal statute.

**(2)** No effect on intellectual property law. Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

**(3)** State law. Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

**(4)** No effect on communications privacy law. Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

**(5)** No effect on sex trafficking law. Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit—

**(A)** any claim in a civil action brought under *section 1595 of title 18, United States Code*, if the conduct underlying the claim constitutes a violation of section 1591 of that title [*18 USCS § 1591*];

**(B)** any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of *section 1591 of title 18, United States Code*; or

**(C)** any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of *section 2421A of title 18, United States Code*, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

**(f) Definitions.** As used in this section:

**(1)** Internet. The term "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

**(2)** Interactive computer service. The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

**(3)** Information content provider. The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

**(4)** Access software provider. The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

**(A)** filter, screen, allow, or disallow content;

**(B)** pick, choose, analyze, or digest content; or

**(C)** transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

## History

**HISTORY:**

June 19, 1934, ch 652, Title II, Part I, § 230, as added Feb. 8, 1996, *P. L. 104-104*, Title V, Subtitle A, § 509, *110 Stat. 137*; Oct. 21, 1998, *P. L. 105-277*, Div C, Title XIV, § 1404(a), *112 Stat. 2681*-739; April 11, 2018, *P. L. 115-164*, § 4(a), *132 Stat. 1254*.

Annotations

## Notes

**HISTORY; ANCILLARY LAWS AND DIRECTIVES**

**References in text:**

**Explanatory notes:**

**Amendment Notes**

**1998.**

**2018.**

**Other provisions:**

**References in text:**

The "Electronic Communications Privacy Act of 1986", referred to in this section, is Act Oct. 21, 1896, *P. L. 99-508*, *100 Stat. 1848*. For full classification of such Act, consult USCS Tables volumes.

**Explanatory notes:**

The bracketed words "subparagraph (A)" have been added in subsec. (c)(2)(B) in order to indicate the reference probably intended by Congress.

Although § 509 of Act Feb. 8, 1996, *P. L. 104-104*, provided for the addition of this section at the end of Title II of the Communications Act of 1934 (*47 USCS §§ 201* et seq.), it was added at the end of Part I of such Title (*47 USCS §§ 201* et seq.) in order to effectuate the probable intent of Congress.

**Amendment Notes**

**1998.**

**Department of Justice**

U.S. Attorney's Office

District of Oregon

FOR IMMEDIATE RELEASE Monday, October 3, 2022

# Oregon Man Charged with Sexually Exploiting Minor on Discord, Additional Victims Sought

PORTLAND, Ore.—An Oregon man has been charged with federal child exploitation crimes after he persuaded a child to engage in a sexually explicit video chat with him on Discord, a popular instant messaging social platform.

Jason Kroeskop, 40, of The Dalles, Oregon, has been charged by criminal complaint with enticing and sexually exploiting a child online.

According to court documents, in August 2022, special agents from Homeland Security Investigations (HSI) in Tulsa, Oklahoma were contacted by local law enforcement to request assistance with an investigation involving the online exploitation of a child under 12. Investigators discovered that Kroeskop pretended to be an Oregon teenager to convince the child to engage in sexually explicit acts during a video chat on Discord. He also recorded the video chat without the victim's knowledge.

Investigators tracked Kroeskop's Discord account, "Noctis Lucis #7347," to an internet protocol address registered to his residence in The Dalles. On September 29, 2022, HSI

special agents from Portland contacted Kroeskop at his place of employment. Kroeskop agreed to talk with the agents and admitted to having engaged in sexually explicit communications with multiple children online since at least 2021 using Discord, Snapchat, and Omegle. He was later arrested without incident.

On September 30, 2022, Kroeskop made his initial appearance in federal court before U.S. Magistrate Judge Jeffrey Armistead. He was detained pending further court proceedings.

This case was investigated by HSI Portland and The Dalles Police Department with assistance from HSI Tulsa. It is being prosecuted by Mira Chernick, Assistant U.S. Attorney for the District of Oregon.

A criminal complaint is only an accusation of a crime, and a defendant is presumed innocent unless and until proven guilty.

Anyone who has information about other crimes committed by Kroeskop, or the physical or online exploitation of any children, are encouraged to contact HSI at (866) 347-2423 or submit a tip online at report.cybertip.org .

Federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor. It is important to remember child sexual abuse material depicts actual crimes being committed against children. Not only do these images and videos document the victims' exploitation and abuse, but when shared across the internet, re-victimize and re-traumatize the child victims each time their abuse is viewed. To learn more, please visit the National Center for Missing & Exploited Children at www.missingkids.org .

This case was brought as part of Project Safe Childhood, a nationwide initiative launched in May 2006 by the Department of Justice to combat the growing epidemic of child sexual exploitation and abuse. For more information about Project Safe Childhood, please visit www.justice.gov/psc.

---

**Topic(s):**
Project Safe Childhood

**Component(s):**
USAO - Oregon

Updated October 3, 2022

**Testimony of Carrie Goldberg**

Founder, C. A. Goldberg, PLLC

**Before the U.S. House of Representatives**

**Committee on Energy and Commerce**

**Subcommittee on Communications and Technology**

**"Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity"**

December 1, 2021

Chair Doyle, Ranking Member Latta and distinguished members of the House Subcommittee on Communications and Technology. Thank you for inviting me to testify today and allowing me to share my experiences representing victims of catastrophic injuries caused by online platforms and the heartbreak of trying to get justice for my clients but being locked out of our courts because of an outdated law, Section 230 of the Communications Decency Act.

My name is Carrie Goldberg. I founded the law firm C.A. Goldberg, PLLC to represent victims of catastrophic injuries – people who've had their privacy invaded, bodies raped, freedoms enslaved, and sometimes lives snuffed out entirely. In the majority of my cases, well over a thousand now, my clients' injuries were facilitated by tech companies. The people -- victims of child sexual exploitation, cyberstalking, trafficking -- hire me as their lawyer expecting me to avenge their damages. The worst part of my job, though is telling people who've suffered horrific nightmares that Congress took away their right to justice. *We can't sue*, I tell them, *Congress passed a law in the 90's that lets tech companies get away with what they did to you*.

This testimony looks at three of my cases, each in different phases of litigation, impacted by the culpable tech companies' claim of immunity, provides some historic context, laments the overreach of our courts in interpretating Section 230, explains why reforming the law will not cause a stampede of litigants to the courts, looks at the four bills being discussed today, and presents a summary and redline of what needs to happen in Section 230 reform to protect the most serious victims and deter the worst of tech's antisocial business practices. My proposal takes bits and pieces from the four proposed bills, as well as recommendations from the Department of Justice's 2020 Symposium about Section 230.

**In summary, we must:**

1. **Remove immunity for Bad Samaritan platforms that purposefully facilitate or solicit criminal conduct or are willfully blind to it;**

2. **Create carve-outs for the most seriously heinous conduct such as child sexual exploitation, terrorism and cyber-stalking and the most serious types of injuries like wrongful death; and**
3. **Eliminate immunity when platforms have actual knowledge of injurious conduct or ignore a court order.**

## I. Intro

I've been vindicating the rights of severely traumatized people since graduating college in 1999. I began my career as a case worker for Nazi Victims and Holocaust Survivors in New York City, providing this dwindling and important group with social services and applying for the various new reparations that materialized in the early 2000's. Suddenly Germany's social security system recognized forced ghetto labor as pensionable. Swiss banks were aggregating lists of dormant accounts from the 1930's and 1940's which were made available on the internet. And there was a new one-shot payment of $2500 for living survivors of concentration camp medical experiments. I was engrossed with the crudeness of assigning money to suffering and how rarely it measured up to the suffering it attached to. I enrolled in law school in the evening, continuing with my Survivors in the daytime. When I graduated with my JD I went on to work at the Vera Institute of Justice where I sued individuals and companies who'd exploited vulnerable people who'd been deemed incapacitated.

In 2014, after narrowly surviving a trauma related to a dangerous individual I met on a dating app, I left my job at Vera and started my law firm to represent victims of online harassment, sexual assault, and personal injuries against big tech. The work was personal and I set out to get restitution and reparations for severe injuries and fatalities to my clients caused in the most modern of war zones, the internet.

Money does not undo injuries or erase traumas. But court's reallocation of money from the injurer to the injured is the best method of justice we have for improving life for victims and deterring future bad acts of offenders. I learned two very important things from the Holocaust Survivors which guide my work at the firm: 1) if somebody hurt you, somebody must pay 2) the only way to stop history from repeating itself is to bear witness and tell the story over and over again until change comes about. That's what I'm here to do today.

I'm one of just a handful of lawyers in the country who litigates against technology companies on behalf of users who've been catastrophically hurt. Section 230 of the Communications Decency Act, that aforementioned law from the 90's, makes it virtually impossible for plaintiffs wounded by tech companies to get beyond the front doors of the court before their case gets tossed to the curb like garbage.

* * * * *

**K.M., a client story**
**Stage: Pre-litigation**

Let me tell you about a Zoom conversation I had with one of my clients and her mother on Friday. K.M. looks sheepish when I ask how she is. She says good and gives her mom the side-eye. Oh, and she hates her new school she just switched to. I tell her I like her new necklace and earrings. After K.M. leaves her bedroom, her mom tells me that K.M. was hospitalized again, this time with fifty pills of Benadryl in her belly. It's her third attempt since I met her in May of 2020. This time it's because an eighteen year old boy said he wanted to hit her after he got in trouble for kissing her at school. Last time it was after confiding that she performed oral sex for somebody on the bus. I ask K.M.'s mom if all this behavior is related to the online exploitation. She says yes, the therapist believes K.M.'s inability to measure sexual risk stemmed directly from that and K.M. was never the same after.

The "that" began in April 2020 when K.M. was 11 years old. She was stuck at home during the most dire stage of New York City's Coronavirus lockdown and met a guy on Instagram who shared her interest in Japanese animè. The guy got K.M. to send him pictures and tell him secrets. Before long, he was coercing and blackmailing her into sending him pictures and videos, dozens of them, of her naked body, masturbating, and inserting objects into her vagina. K.M. would stay up all night in the bathroom, so she wouldn't wake her sister, doing what he wanted. The offender direct messaged K.M. about obscene things, making her agree to plans of incest and gangbangs on their future children. Using all this material, the offender coerced K.M. into sharing the passwords to her Instagram accounts. After not sending him the 150 nudes he demanded one night, the offender attempted to post nude images of K.M. publicly onto her Instagram Story. Locked out of her account and unable to stop him, K.M. received a notification on her phone saying images were blocked from being posted on her Story because of inappropriateness. Instagram seemingly identified nude images coming from a child's account and prevented them from being posted. The offender shifted gears and began distributing the images from K.M.'s account to K.M.'s followers by direct message. Instagram did not block the image when disseminated through direct message, despite earlier saying it knew it was a child's account. K.M.'s account sent it to sixteen people, fifteen of whom K.M. knew personally, and twelve of whom were young teenagers. When K.M.'s aunt told her sister (K.M.'s mom) she'd received these images of K.M., K.M.'s mom immediately tried to find the phone number for Instagram. She went on the website and frantically googled the company, but couldn't find a phone number or email address. K.M.'s mom, an immigrant from Guatemala who cleaned houses for a living did not herself have an Instagram account. Her daughter remained locked out of the account. The guy still had control. Desperate, K.M.'s mom took her to the police precinct where the reporting officer lectured them that they ought to learn the difference between "discipline and crime" before sending them on their way.

K.M. was forced to transfer schools because she was too humiliated to even be in Zoom class with the other kids. K.M. was unable to cope with the shame. She suffers from extreme guilt for putting her family through this experience. She says she feels like everybody thinks she's disgusting and that she's ruined her family. Her father moved out of the house and their dog died one after the other. She began cutting herself and says she feels dead at times. At some point, either after the first or second hospitalization for suicide attempt, child protective services opened a negligence case against K.M.'s mom for leaving her daughter unattended for short spurts while she cleaned houses. This will be on her permanent record until K.M. is 28 years old and will impact her immigration status. K.M.'s mom is down to three half-day cleaning shifts a week and was forced to put the family on welfare. She could go to jail if she is caught leaving K.M. alone again. They can't afford to live.

* * * * *

I've not yet brought claims for K.M. Litigation would be too stressful for her at this point and could lead to another suicide attempt. An attempt, or worse. Facebook/Instagram (sorry, I refer to indulge their rebrand or buy into a new dimension they are putting a stake in) make a show of advertising online and on television that they want reform and regulation. However, it's smoke and mirrors. In reality, they still parade around saying they are immune from liability both in litigation and pre-litigation settlements because of Section 230 and refuse all responsibilities for injuries they cause to people like K.M. When I think of Section 230 reform, it's through the litmus test of whether it will vindicate K.M.

## II. Section 230, how we got here

In 1995, Congress passed 47 U.S.C. Section 230 as part of the Communications Decency Act. It was a small section of a broader bill intended to combat pornography on the internet which lawmakers realized children were accessing. Section 230 established protections for websites from being sued for publication torts like defamation for content their users post. At the time, the main source of user-generated content was online bulletin boards, Prodigy and AOL, where the most heinous acts of the day, comparatively mild to the destruction now, were people calling each other frauds. One court had found that a bulletin board was liable for defamatory content one user posted about another, because that bulletin board had been actively moderating the content on its site.

In the mid-1990's haze of deregulation, Congress speculated that if bulletin boards were freed from liability to their users, they'd self-moderate and voluntarily implement measures to keep their platforms and users safe. The idea was that removing the threat of liability would *incentivize* these companies to be good Samaritans and self-govern their platforms responsibly.

That is not what happened. Just as when Wall Street was deregulated, without rules, regulation or the threat of lawsuits from injured users, the companies ran amuck. They could grow at quantum speed without the need to invest any money into keeping their product safe or establishing responsible policies and procedures to respond to injuries or staffing moderators in scale with the number of users on their platforms. Rather than incentivizing good content moderation hygiene, Section 230 became a shield for platforms, and a license to get away with no content moderation or safety measures.

Concurrently, an overhaul of internet companies' revenue model – from subscription to "free" -- was the nail in the coffin for online consumer safety. What had once been subscription-based model with users paying monthly fees to companies like AOL in the 90's transformed into an advertisement-based model. Users were no longer the customers; advertisers were. No longer did companies need to compete to provide the best service to their users. When Internet products became "free" to users, users went from being valued customers to the commodity, the eyeballs on the ads. The coldshoulder to users' needs and safety has become far more extreme in today's internet

where users are not just the commodity to advertise at, but instead are the raw material from which companies like Facebook, Google, and Amazon extract behavioral and consumer data, then use it to manipulate and forecast those very same users' habits.

Ironically, my clients, especially my exploited underage clients, are the ones that the 1995 Congress was trying to protect. Yet, this is the population most victimized by the creep of immunity.

Over past 25 years, our courts took a rather narrowly written law which was intended only to prevent lawsuits against tech companies related to publication torts, like defamation and obscenity, and metastasized it into shielding the most powerful companies in the world from responsibility for things like terrorism, genocide, child sexual exploitation, illegal firearms dealing, and stalking. It expanded the law well beyond claims of defamation and obscenity, to also throw plaintiffs out of court if they claimed their injuries were caused by negligence, fraud, contract breaches from companies violating the terms of service agreements, discrimination in advertisements, and the product being detective. Even statutory damages in our federal child pornography law is off-limits for survivors despite companies making a profit off their nude images.

The tech industry is not inherently bad. As David Michaels explains in his book, "The Triumph of Doubt" about cover-ups in toxic torts, most problematic corporate behavior happens through a series of small decisions. Publicly traded and investor-based companies are pressured to deliver growing profits on a short-term basis. The culture of angel investors and venture capitalists hungry for that next unicorn normalizes this dangerous "move fast and break things" ethos. Unfortunately, the broken things are too often living breathing humans. Milton Friedman's fetishized model that a corporation's primary objective is to maximize shareholder value, even presenting it as a fiduciary responsibility limited only by the boundaries of law and regulation. So when there's neither law nor regulation, and the injured are excluded from our courts to vindicate their harms, the products get more dangerous and the corporate greed more deeply rooted.

The importance of litigation to discourage corporations, entire industries even, from their most antisocial temptations. When the ill effects of a dangerous or toxic product shift the true costs of those products onto humans and communities, litigation is how we boomerang those costs right back to the source. This "regulation by litigation" is how our society took on Big Tobacco, opioid manufacturers, asbestos, carcinogenic weedkillers, massive polluters, and more. The process of litigation, even when the defendants engaged in evasion, obfuscation, and cover-ups have provided critical inside reports and insights into the level of recklessness with which the industries knew they were injuring the community. Without litigation, we must rely on the whitewashed dribs and drabs of "transparency reports that tech PR flacks deign to release to the public or wait for a rare whistleblowers like Frances Haugen to leak internal documents at tremendous personal risk.

* * * * *

**Matthew Herrick: A client story**
**Stage: Post-litigation**

It all started one evening in late October 2016, right before Halloween. Matthew sits on the front stoop of his New York City apartment, smoking a cigarette, when a stranger calls to him from the sidewalk and starts heading up the steps toward him. The stranger's tone is friendly and familiar. But Matthew has never met this guy before. "I'm sorry," he says. "Do I know you?"
The stranger raises his eyebrows and pulled his phone from his back pocket. "You were just texting to me, dude," he replies, holding out his phone for Matthew to see. On the screen is a profile from the gay dating app Grindr, featuring a shirtless photo of Matthew standing in his kitchen, smiling broadly.

The stranger keeps holding up his phone, insisting Matthew had invited him over for sex. But Matthew knows the profile isn't his. Finally, the stranger becomes exasperated and leaves. "Fucking liar!" he shouts in Matthew's direction as he walks away. "You're an asshole!"
Rattled, Matthew goes back inside. A few minutes later, he hears his buzzer ring. It's another man insisting that he, too, had made a sex date with Matthew. Two more men show up that day. And three others came calling the next. "Matt!" they holler from the sidewalk, or they'd lean on the buzzer expecting to be let in. At first the strangers only go to his apartment, but by the end of the week a steady stream of men are showing up at the restaurant where Matthew works as well. Some in their 20s, others much older. A few arrive in business suits, as though on the way to the office. Others are twitchy and sweaty, looking like they'd been up all night getting high. They'd stalk him at work and at home, all hours of the day and night, each one convinced Matthew had invited him over for sex.

Matthew knew his ex was behind the strangers – they began showing up a week after their break up. The impersonating profiles sent men for fisting, orgies and aggressive sex. In the direct messages, the strangers were told that Matt's resistance was part of the fantasy. Like many of my clients, before coming to see me Matthew had tried everything he could to take care of the problem on his own. He filed more than a dozen complaints with his local police precinct. The officers dutifully took down his information but didn't seem to understand the danger he was in.

By the time Matthew came to me for help, the Manhattan district attorney opened an investigation and he'd gotten a family court "stay away" order, but neither was stopping the traffic of strangers coming to his home and work for sex. He also did everything he could to get the imposter profiles taken down. He directly contacted Grindr and its competitor Scruff, which Matthew's ex was also using to impersonate him. In their terms of service, both companies explicitly prohibit the use of their products to impersonate, stalk, harass or threaten. Scruff, the smaller of the two companies, responded to Matthew immediately. It sent him a personal email expressing concern, took down the fake accounts, and blocked the ex's IP address, effectively banning him from the app. When the ex started impersonating Matthew on Jack'd, yet another gay dating app, that company also banned him from using its platform to harass Matthew. But Grindr took a different approach: It did absolutely nothing.

In all, about 50 separate complaints were made to the company reporting the fake profiles, either by Matthew or on his behalf. The only response the company ever sent was an automatically generated email: "Thank you for your report." Over the course of ten months more than 1,400 men, as many as 23 in a day, arrived in person at Matthew's home and job.

Grindr is a wildly successful company. In 2018, the dating app reportedly had more than three million users in 234 countries. Like most social media companies, Grindr operates, in large part, as an advertising platform. The free content and services these platforms provide—porn, photo sharing, direct messaging, emailing, shopping, news, dating—are really just lures to get people

to show up so the companies can collect data about what users buy, who they're friends with and where they're going, and use that information to advertise. Grindr prides itself on its state-of-the-art geolocative feature, which can pinpoint a user's exact location, allowing users to match with others in their vicinity. This is how they rake in advertising revenue—by customizing the ads that users see based on nearby businesses.

Even though Grindr's terms of service state that Grindr can remove any profile and deny anybody the use of their product at the company's discretion, they refused to help. After Matthew's approximately 50 pleas to Grindr for help were ignored, we sued Grindr in New York State Supreme Court, New York County, and obtained immediate injunctive relief requiring that Grindr ban the malicious user.

It's not clear exactly how Grindr was so easily being used to send the strangers to Matthew—it might have been through a spoofing app that worked with Grindr's geolocation software or something more technical. But the strangers who came to Matthew said they were sent through the Grindr app and would show Matthew the fake profiles with his pictures, geolocation maps showing how far away they were from Matthew, and direct messages telling them which buzzer to ring and what kind of sex Matthew was eager to have.

I didn't need to explain on a technical level how Grindr was being used against Matthew at this stage of the litigation; that's what discovery is for. What we knew is that Grindr was in an exclusive role to help stop Matthew's hell, given law enforcement was too slow and the ex had been deterred by neither arrests nor orders of protection.

I knew from the start that Grindr would claim it was immune from liability pursuant to Section 230 of the Communications Decency Act, which states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

So I made sure not to sue Grindr for traditional publication torts like defamation. That is, I was not suing them for any words the ex said on the profiles or communications he'd made on the app. Instead, I tried something new—I sued Grindr using traditional product liability torts. I argued that Grindr is a defectively designed and manufactured product insofar as it was easily exploited—presumably by spoofing apps available from Google and Apple—and didn't have the ability, according to the courtroom admissions of Grindr's own lawyers, to identify and exclude abusive users. For a company that served millions of people globally and used geolocating technology to direct those people into offline encounters, it was an arithmetic certainty that at least some of the time the product would be used by abusers, stalkers, predators and rapists. Failing to manufacture the product with safeguards for those inevitabilities, I argued, was negligent.

On Feb. 8, 2017, Grindr filed a notice of removal from state court to the Southern District of New York. Our temporary restraining order requiring that Grindr ban the ex from its services expired as a matter of law 14 days after the removal—but when we moved to extend the order, Judge Valerie Caproni denied the extension. Judge Caproni felt our underlying case lacked merit because she suspected Grindr was immune from liability pursuant to the Communications Decency Act, arguing that our claims depended on information provided by another information content provider. If not for Matthew's ex using the app, she reasoned, none of this would have happened to Matthew. She reduced all the harm as flowing from the ex's actions, not Grindr's, and therefore reasoned that the company was immune from liability and had no obligation to Matthew. In April and May of 2017, Grindr and its holding companies filed motions to dismiss our claims. At the time, Matthew's ex was continuing to relentlessly use the app to send strangers to his home and job—a fact the court knew.

We argued in our opposition papers that because we were suing Grindr for its own product defects, operational failures and broken promises in their terms of service—and not for any content

provided by Matthew's ex—Grindr was not eligible to seek safe harbor from Section 230. To rule against Matthew would set a dangerous precedent, establishing that as long as a tech company's product was turned to malicious purposes by a user, no matter how foreseeable the malicious use, that tech company was beyond the reach of the law and tort system.

Nevertheless, on Jan. 25, 2018 Judge Caproni dismissed our complaint entirely. All but a copyright claim was dismissed with prejudice, meaning that even if Matthew learned new information to support his claims, he could not amend his complaint.

Matthew's case was thrown out before we'd even gotten our foot in the door—even though dismissal at the motion to dismiss stage is supposed to be reserved for situations where a complaint is defective on its face, while ours was a detailed, thorough 43 pages and well-pleaded. The judge relied on Grindr's immunity under Section 230.

To our disappointment, on March 27, 2019 the Second Circuit issued a summary order affirming the district court's dismissal of the complaint. On April 11, we filed a petition for panel rehearing, or, in the alternative, for rehearing *en banc*. On May 9, that too was denied. In October 2019, our writ for certiorari, also was denied. It was the end of the road for *Herrick v Grindr*.

* * * * *

The Supreme Court has never ruled on the proper scope of Section 230. As Matthew's case demonstrates, this is a matter of life or death for victims of stalking and violence caused and exacerbated by computer technologies unimagined when Congress passed the law in 1996. Decades ago, lawmakers had this pie-in-the-sky idea that internet companies would monitor content their users uploaded to protect the rest of us. What's become painfully apparent, and arguably should have been obvious, is that without the threat of legal liability hanging over their heads, companies like Grindr really don't care about who gets hurt.

In 2020 Justice Clarence Thomas wrote a dissent to a writ for certiorari in the case Malware Bytes, Inc. v Enigma Software Group. He lamented that when Congress enacted Section 230, most of today's major Internet platforms did not exist. Then he condemned how the two and a half decades of lower court decision "eviscerated the narrow liability shield" Congress had intended. Making his point, he cited Matthew's case, furious that courts so extravagantly interpreted Section 230 that it even granted immunity in a product liability case "concerning a dating application that allegedly lacked basic safety features to prevent harassment and impersonation."

Fortunately, our product liability theory has been advancing places outside the 2nd Circuit. In 2021's *Lemmon v Snap*, the 9th Circuit said Snap was not immune from liability for one of its features, an app filter which the court said encouraged kids to drive fast. Consequently, the plaintiffs may move forward with their theory of liability that the feature contributed to the deaths of the young men using the filter and crashed their car at 120 mph.

## III. The Court's Too Broad Interpretations of Section 230

Joining Herrick v Grindr in the court's broadening interpretation of section 230 are the following:

- *Dyroff v. Ultimate Software Group, Inc.*, 934 F.3d 1093 (9th Cir. 2019), the Court held that there was no material contribution when a website connected two users to each other based on the free- form comments they wrote on the site about their interest in heroin. A teenager died of fentanyl poisoning after the other user sold him fentanyl instead of heroin.

- *Force v. Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2020), the Court held that Facebook did not materially contribute to illegal content where its algorithm amplified terrorist content. Arranging and displaying third party user's content to others was not material contribution.

- *Jane Doe No. 1 v. Backpage.com LLC*, 817 F.3d 12 (1st Cir. 2017). There, sex-trafficking victims sued Backpage.com, a classifieds hub that (among other things) hosts online advertising for illegal commercial sex in the United States. Even though the plaintiffs had marshaled persuasive evidence that Backpage.com had adopted rules and practices that facilitated sex trafficking—from selectively removing postings discouraging sex trafficking and tailoring its rules to protect sex trafficking from detection to removing metadata on photographs—the First Circuit concluded that Backpage was entitled to Section 230 immunity. This led to a Congressional amendment.

- *Goddard v. Google, Inc.,* 640 F. Supp. 2d 1193, 1196 (N.D. Cal. 2009). There, the plaintiffs alleged that Google's Keyword Tool suggested words to include in advertisers' ads and often added words that resulted in false advertisements (such as turning the word "free" into "free ringtone" even though the advertised service would not be free). But the district court concluded that the Keyword Tool was a "neutral tool" that had immunity—even though Google had itself suggested the false phrases that advertisers had used in their ads

- *Fields v. Twitter, Inc.,* 217 F. Supp. 3d 1116 (N.D. Cal. 2016). There, the plaintiffs argued that Twitter's provision of accounts—which ISIS members then used to communicate with one another, recruit members, and spread propaganda—amounted to providing material support for terrorism. See id. at 1119. But the district court found Twitter categorically immune under Section 230. According to the court, giving ISIS members Twitter accounts was "publishing activity" for Section 230(c)(1) purposes because handing out accounts necessarily "include[s] decisions about what third-party content may be posted online."

## IV. Removing Section 230 immunity will not flood the courts.

Removing the exemption of liability will not result in a groundswell of litigation. In discussing Section 230 reform, some people erroneously claim changes to 230 will "create liability" for tech companies. This is incorrect. Removal of immunity will not

make defendants liable for online harms. Instead, it just means plaintiffs have a chance to prove their claims in the first place. Fears that tech companies will be overwhelmed with litigation are unfounded and frankly, reveal the fearmonger's unfamiliarity with how litigation works. In this section I discuss why we need not fear a stampede to the courthouse.

*The onus is on the plaintiff to prove liability.*

Like all litigation, the onus is on the plaintiff to *prove* the merits of the case and the plaintiff will sometimes fail. The process begins with plaintiffs needing to satisfy the harsh pleading standards required of federal cases per *Iqbal* and *Twombly*. The plaintiff must have an actual cause of action to plead and then must plausibly plead each element. For instance, if pleading negligence, the plaintiff must plead that there's a relationship between the plaintiff and the defendant, that the relationship created a special duty on defendant, that defendant breached that duty, that plaintiff suffered an injury, and that the defendant's breached duty was the proximate cause of the injury.

*Basic economics deter low injury cases*

Proving liability is an arduous, laborious, years-long and expensive undertaking for plaintiffs and/or their attorney. Economic drivers separate the wheat from the shaft. Personal injury cases are almost always taken on contingency. Rare is the client with millions of dollars to fund cases against tech. Discovery, expert witnesses, depositions, and thousands of hours of lawyer time adds up. Likewise, attorneys working on contingency with their own profit and loss concerns do not take cases unless the upside justifies the risk of losing litigation. My tiny firm spent over a million dollars of lawyer time losing Matthew's case. Consequently, frivolous and low injury cases are eliminated before they're ever filed.

*Having facts that satisfy all elements for a cause of action is surprisingly difficult*

Weak cases where there is nominal injury and weak facts about content moderation will be dismissed at as early a stage as if there were immunity. For instance, somebody being called a "bitch" on Twitter would never succeed with a negligence claim and it would be dismissed at no earlier a stage than the 12(b)(6) motion to dismiss stage used by tech companies presently. Take another example of the often catch-all cause of action but with a very high bar, intentional infliction of emotional distress. The elements of this claim require a plaintiff plead a defendant acted intentionally or recklessly, the defendant's conduct was extreme and outrageous, the defendant's act is the cause of distress, and the plaintiff suffers severe emotional distress as a result. Let's say a politician sues Facebook for intentional infliction of emotional distress for removing a post that encourages violence. Facebook could easily argue that its decision to moderate its content was neither extreme nor outrageous nor that it caused emotional distress, let alone severe emotional distress.

*Nothing will be procedurally different for defendants without Section 230 because rarely do they rely on Section 230 alone.*

Without Section 230 immunity, nothing would procedurally change for tech companies in getting weak cases dismissed. Tech companies usually make initial (pre-discovery) motions to dismiss based on a variety of grounds, including failure to state a claim, Section 230 immunity, outside the statute of limitations, lack of jurisdiction, and anti-SLAPP. Poor cases will be dismissed at this early stage and before the rigors of discovery.

*Anti-SLAPP laws are a faster and harsher deterrent for Defendants to get weak and constitutionally protected speech-based claims dismissed.*

Plaintiffs bringing frivolous content-based cases like the two described above (negligence claim for being called a bitch on Twitter and IIED claim for a platform removing inciting contet) are far more deterred by Anti-SLAPP laws than section 230. Strategic Lawsuits Against Public Participation (SLAPP) provide an accelerated and even profitable way for defendants to get flimsy cases thrown out. Thirty four states have anti-SLAPP laws. Written into many Anti-SLAPP statutes is a condensed briefing schedule, and the requirement that courts prioritize these cases. Anti-SLAPP statutes create a two-prong test. A defendant must show they're being sued for constitutionally protected speech and then the burden passes to the plaintiff who must show a likelihood of success of winning on the merits of their case. Because Anti-SLAPP motions occur before discovery and it's up to the court's discretion as to whether to allow limited discovery in these motions, plaintiffs are already at a huge disadvantage because the second prong requires a mini trial wherein plaintiffs must provide evidence that they can meet the elements of the cause of action but without the plaintiff having the benefit of discovery. The biggest source of deterrent is the required fee-shifting. A plaintiff who loses their anti-SLAPP motion must pay the defendant's legal and fees. Legal fees typically add up to six figures in Anti-SLAPP motions.

The two examples discussed above – the negligence case based on rude behavior and the IIED case about a moderation decision – if brought against an Interactive Computer Service (ICS) would both most certainly be dismissed in an Anti-SLAPP motion and the plaintiff could expect to be forced to pay punishing legal fees for both their own attorney and the defendant's.

*Uninformed plaintiffs sue anyway*

Section 230 immunity already does not deter pro se litigants with truly frivolous cases. Folks hellbent on suing will sue with or without the immunity and likely will not even learn of Section 230 immunity until their case is already being dismissed.

*Proving psychological injuries is challenging*

The majority of cases against big tech involve psychological – and not physical injuries. Proving a psychological injury can be more challenging than a physical one. While there are photographs, x-rays, and courtroom three-dimensional models that aid in proving physical damages, often victims of emotional distress keep the full extent of their injury private. The victim is responsible for describing their emotional injury and eliciting

empathy from the jurors who may well blame them. Defendants have an easier time sowing doubt in a jury, claiming the victim is at fault or is lying or exaggerating the harm or that earlier or later traumas caused the anguish. Because the claims are far more difficult to prove, lawyers are disincentivized from taking anything but the most egregious cases.

*Will the ICS really be paying for claims itself?*

All responsible businesses have liability insurance. It would be shocking if a user-facing platform did not have an insurance policy to deal with lawsuits. I suspect the biggest impact of removing Section 230 immunity will play out in the world of insurance.

* * * * *

**A.M: A client story**
**Stage: In litigation, filed November 19, 2021**

He is 37.
She is 11.
They both are on the site Omegle.
The banner up top says "talk to strangers."
Omegle matches the two to video chat.
The man comforts her in her 11 yo loneliness.
At first he wants to see her smile.
Then he asks her to show another body part.
And another *and another* .
She does protest. And he says you're free to stop. But alas, I'd have no choice but to send these videos to your parents and friends at school. And the police. You don't want to get in trouble do you? You've created child pornography and will go to jail.
This goes on for 3 years.
He makes her perform for he and his friends. He forces her to recruit more kids on Omegle.
One day an FBI agent contacts A.M.'s parents. They say they tracked them down after Canadian police did a raid on a man's home, a home he shared with his wife's daycare business. And they discovered 3000 files of porn, including several hundred of a young girl. In one, that young girl is wearing a sweatshirt with the name of the same school A.M. attends. The school recognized her as A.M.
Just like that, her nightmare ended. Except it didn't. Ever since, A.M. suffered extreme social anxiety, panic attacks, and breakdowns. She was still convinced that he would kidnap her or have her arrested. At first, she'd wanted to go to his aid.

* * * * *

We filed A.M.'s lawsuit against Omegle ten days ago. The media was full of stories of children being preyed upon by predators on this platform, including one BBC article where the journalists went undercover and were astonished by the number of both

masturbating children and adults they were randomly matched with, it being apparent that adults were there for one extremely disturbing purpose. Like in Matthew's case, the heart of the claims is that it was a defective product in that it is clearly used by children and adults for sex videochatting, yet does nothing to separate the two populations. Judging by its track record, Omegle will say it's her fault and that it says right there on its site that it's for kids 13 and older, as if the outcome would have been any different if she'd been two years older. Omegle will say they are free to pair adults and children and have no duty to prevent abusers, that Section 230 protects them from lawsuits like this.

## V. The four reform proposals on the table today

The four proposed bills discussed at today's hearing are a step in the right direction toward correcting the overbreadth our courts interpreted into Section 230. Each of them contains laudable elements.

The Civil Rights Modernization Act of 2021 (H.R. 3184) removes the liability exemption for targeted ads that discriminate. This is important because companies should not be immune from liability for content like ads they profit from. I'd take it steps further, in my opinion, the monetization of content ought to transform the Interactive Computer Service into an Information Content Provider with relation to said content. Alternatively, with paid content, the platform is not truly performing the role of an Interactive Computer Service, but rather the role of a billboard or marketer. Narrowing the definition of ICSs and ICPs accordingly to address when paid content transforms these designations is a more expansive way to address the issue. Lastly the CRMA only applies to claims pertaining to injuries stemming from civil rights violations. Unfortunately, this would exclude the most vicious harms and serious injuries we see online which are not typically based on discrimination, but violence.

The Protecting Americans from Dangerous Algorithms (H.R. 2154) smartly and appropriately classifies algorithms as ICP. This law is so narrow as to be almost unusable. It excludes so many presentations of algorithms (i.e. ranked, ordered, promoted, recommended, amplified, or altered in a way that is obvious, understandable and transparent to a reasonable user, chronologically listed, sorted by user ratings or numbers of reviews, alphabetical, random, organized by views, downloads or similar.). It applies only to large companies which is a disappointing delimiter since some of the most deliberately malicious platforms are small. Oddly, it rules out all claims except those pertaining to equal rights and injuries from international terrorism. My clients would stand no benefit.

The Justice Against Malicious Algorithms Act (H.R. 5596) is a far superior way to address injuries caused by algorithms than H.R. 2154. This bill creates a new exception to immunity for suits against ICS' for injuries caused from algorithmically directing a user to material that causes them injury. I could envision this applying to scenarios exposed recently such as Instagram directing teen age girls to thinspiration and weightloss content and playing a causal role in the eating disorders that result. I further envision this benefitting my clients who are matched through dating apps with dangerous individuals, such as my client, Matthew Herrick. I do fear that the exception

to the exception for user-specified searches will create a sinkhole many worthy plaintiffs will fall into. I also recommend against the narrowing mens rea requiring the ICS "knew or should have known" or "acted recklessly." These will be abused by defendants an overinterpreted by courts. Lastly, injuries ought not be limited to "physical or severe emotional injury." Although most of my clients do suffer severe emotional injury, we must not overlook financial injuries and the like.

The Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act ("SAFE TECH Act**")** (H.R. 3421), of the four bills, this one will vindicate the injuries I deal with the most. First, in (c)(1) it changes the immunity from applying to "any information" provided by a third party to "any speech" provided by a third party. Hopefully courts will recognize this as an attempt to for courts to start distinguishing between content (immune) and conduct-based (hopefully not immune) harms.

SAFE TECH also removes immunity for speech that the ICS profited from or funded. As I have long advocated, this bill requires that 230 immunity be an affirmative defense for which the defendant has the burden of persuasion. This has the advantage of unburdening the court with having to play computer scientist in a 12(b)(6) decision, determining without facts from the defendant that they are in fact an ICS being treated as the publisher or speaker of information provided by another ICP. Other excellent provisions of SAFETECH include the immunity exclusion for injunctive relief which is important when a victims' main concern is getting illegal material such as nonconsensual pornography or child sexual exploitation material off the web site. Finally, it creates five new categories of carve-outs: claims relating to 1) civil rights laws, 2) antitrust laws, 3) stalking, harassment or intimidation laws, 4) international human rights laws, and 5) wrongful death actions.

The carve-outs are good, especially in that they apply to both state and federal laws but require some tweaking of the language in order to be useable by injured plaintiffs in litigation. Most specifically we need the carve-outs to apply to the facts and not laws. A technical point, but an important one. Many crimes, such as stalking, harassment, human rights abuses, do not have a private right of action. That is, victims can't sue for the violation of these laws, but rather must use classic tort law to make their claim. For instance, my stalking clients in New York could not bring a lawsuit against their stalker or a platform that facilitated the stalking because there is no private right of action for stalking. Stalking is only a criminal law. Instead, a victim would sue the platform for negligence or breach of contract or negligent infliction of emotional distress. We also must eliminate the delimiter on the stalking, harassment and intimidation carve-out which requires "in whole or in part" that the harmful conduct be based on a protected class (i.e. sex (including sexual orientation and gender identity), race, color, religion, ancestry, national origin, physical or mental disability")

## VI. Carrie's fix

We have a real mess here, but a fixable one. Congress created Section 230 and has the power to fix it. Any proposals for reform I consider through the lens of the most wrenching harms I see in my office. **Any legislation must distinguish between**

**hosting defamatory content versus enabling criminal conduct. The first deserves 230, the second does not.** In addition to the three clients I described in detail here (K.M., Matthew Herrick, and A.M.) here, reform must provide paths to justice for the following clients, a small sample of our cases, who've suffered devastating injuries:

- The family of a 27-year-old man who was directed to Amazon.com from a pro-suicide website and sold sodium nitrite, delivered by Amazon Prime, he killed himself two days later. In the middle of the suicide, he indicated he didn't want to die but it was too late. Amazon removed user reviews, manipulates the star rating, refused to put known warnings on the bottle or its website which should have contained an effective way to reverse the effects (methylene-blue), and strategically cropped photos of the product against its own terms of service to exclude the warning label. We've spoken to four other families who lost a loved one from Sodium Nitrite purchased on Amazon.
- The families of seven children who were each sold one fentanyl-laced pill on Snap. All died. The youngest child was 14, a skateboarding phenom. Snap has refused to crackdown on the Fentanyl murders it's facilitating despite the United States hitting its all time record for drug overdoses in 2020, largely because of Fentanyl.
- The family of Bianca Devins whose murder was liveposted on Instagram. Instagram facilitated the spread of her murder images by refusing to remove the murderer's account. Its explanation? They said they needed confirmation the account did not instead belong to somebody impersonating the murderer. To date, Instagram refuses to give Bianca's family control over her account despite acknowledging it's an asset of the estate. Her family is consistently harassed online and taunted with murder images of Bianca, which Instagram is seemingly unable to hash and remove. Recently, somebody sent Bianca's mom a murder image of Bianca covered in ejaculate.
- The family of Alison Parker, a beautiful and young newscaster who was shot dead on the air. YouTube is unable or unwilling to get the content removed from its platform and the news corporation refuses to transfer copyright of the footage to the family so they can sue YouTube/Google for infringing its copyright (one of the few causes of action the drafters did create an immunity exception for in 1995)
- The young woman who was barely eighteen when she was coerced into filming a very graphic pornography video with three men double her age. After a painstaking negotiation, she purchased copyright from the offenders, but websites, including Google refuse to honor her content removal requests which comply with the Digital Millenium Copyright Act. Unfortunately, a copyright suit will create more attention to the content in question and Google which continues to rank the images high in her search engine results, should be liable not just for intellectual property violations, but for its algorithmic negligence.

Short of eradicating Section 230 my recommendations are most similar to the Key Takeaways and Recommendations published by the Department of Justice in June 2020 after its February 2020 symposium "Section 230 – Nurturing Innovation or Fostering Unaccountability." I was relieved to see many of my own recommendations from that

event adopted by DOJ. These recommendations recognize that large tech platforms are no longer nascent or fragile, if ever they were, preserves competition, and keeps core immunity for defamation to foster free speech.

- Conduct carve-outs
  - Bad Samaritan carve-outs – no immunity from civil liability for platforms that
    - purposefully facilitate or solicit third party content or activity that violates criminal law;
    - Are willfully blind to illicit conduct, (e.g. failure to detect or respond to illegal conduct, preventing or seriously inhibiting swift detection and banning of offenders, impeding law enforcement's ability to investigate and prosecute serious crimes, and depriving victims of the evidence they need to bring civil claims against their perpetrator)
  - Egregious conduct carve-outs – no immunity for the worst type of conduct -- claims involving child exploitation, sexual abuse, terrorism, and stalking. Section 230 was never intended to shield platforms from liability so far outside the original purpose of the statute
  - Actual knowledge and court judgments – no immunity where a platform has actual knowledge or notice that the third party content violates criminal law or ignores a court order indicating that content is unlawful or that published content or conduct on a platform underlies a criminal case or civil restraining order.
- Injunctive relief to help in emergency cases where the plaintiff is suffering imminent harm because of harms on a platform or a court has ruled content unlawful or when the basis of a criminal case or civil restraining order is content or conduct occurring on a platform
- The ICS is the ICP and therefore not entitled to immunity for claims pertaining to
  - Breaches of its own terms of services;
  - Breached promises made to users or the public;
  - Testimony of its executives under oath;
  - Constructive notice of the specific harm and damages; or
  - Paid content, including in-kind payment. This includes payment to or from the ICS;
  - Content recommended to users via algorithm;
  - Defectively designed or manufactured products or failure to warn;
- Define "information content" to include only speech-based content
- Limit immunity to only publication-related torts like obscenity and defamation.

For a full redline version of my proposed reform, the Herrick Act Against Violence Online ("HAAVO"), please see Exhibit A.

## VII. Conclusion

What is illegal online, should be illegal offline. Americans are being injured by tech companies running amuck, unconstrained by regulation, liability for their product, or

the threat of litigation. Everyday people lost their fundamental right to the courts to vindicate their injuries. This has created an undeserved windfall for the tech industry, allowing it to become the most powerful, wealthy, omnipotent, and omniscient industry in the history of the world. The trio of corporations, courts, and Congress birthed a monster. Through legislative reform, Congress can fix what corporations won't because of greed and court's can't because of bad accumulated case law. Anybody could become my next client.

EXHIBIT A

A BILL

To amend Section 230 of the Communications Act of 1934 to reaffirm victims' rights and consumer protections.

SHORT TITLE

This Act may be cited as the Herrick Act Against Violence Online ("HAAVO")

(c) PROTECTION FOR "GOOD SAMARITAN" BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.

(1) TREATMENT OF PUBLISHER OR SPEAKER. (A) No provider or user of an interactive computer service shall be treated as the publisher or speaker of any ~~information~~ speech provided by another ~~information~~ speech content provider.

(2) CIVIL LIABILITY. No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, promoting terrorism or violent extremism, harassing, promoting self-harm, or unlawful, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in Subparagraph (1).

(d) EXCLUSION FROM "GOOD SAMARITAN" IMMUNITY.

(1) "BAD SAMARITAN" CARVE-OUT. Subsection (c)(1) shall not apply in any criminal prosecution under State law or any State or Federal civil action brought against an interactive computer service provider if, at the time of the facts giving rise to the prosecution or action, the service provider acted purposefully with the conscious object to promote, solicit, or facilitate material or activity by another content provider that the service provider knew or had reason to believe would violate Federal criminal law, if knowingly disseminated or engaged in.

(2) CARVE-OUT FOR ACTUAL NOTICE OF FEDERAL CRIMINAL MATERIAL. Subsection (c)(1) shall not apply in a criminal prosecution under State law or any state or Federal civil action brought against an interactive computer service provider if—

17

Goldberg, Holding Big Tech Accountable, Dec. 1, 2021

(A) such prosecution or action arises out of a specific instance of material or activity on the service that would, if knowingly disseminated or engaged in, violate Federal criminal law;
(B) the provider had actual notice of that material's or activity's presence on the service and its illegality; and
(C) the provider failed to do any of the following:
(i) expeditiously remove, restrict access to or availability of, or prevent dissemination of the specific instance of material and take reasonable steps to remove, restrict access to or availability of, or prevent dissemination of the material across the service;
(ii) thereafter report the material or activity to law enforcement when required by law or as otherwise necessary to prevent imminent harm; or
(iii) preserve evidence related to the material or activity for at least 1 year.

(3) JUDICIAL-DECISION CARVE-OUT. Subsections (c)(1) and (2) shall not apply in any criminal prosecution or civil action or injunction arising from the failure of an interactive computer service provider to remove, restrict access or availability to, or prevent dissemination of material within a reasonable time after receiving notice of a final judgment from a court in the United States indicating that such material or activity is defamatory under state law or unlawful in any respect. However, no interactive computer service provider shall be held liable for removing, restricting access to, or preventing dissemination of material in response to receiving such notice.

(4) NOTICE MECHANISM REQUIREMENT. An interactive computer service provider shall make available to the public, without expense, an easily accessible and apparent mechanism for notifying the provider of defamatory or unlawful material or activity as described in Subsections (d)(2) and (3). An interactive computer service provider shall not be entitled to assert immunity under Subsection (c)(1) if it designs or operates its service to avoid receiving actual notice of Federal criminal material on its service or the ability to comply with the requirements under Subsection (d)(2)(C).

~~(d)~~ (e) OBLIGATIONS OF INTERACTIVE COMPUTER SERVICE. A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

~~(e)~~ (f) EFFECT ON OTHER LAWS.

(1) NO EFFECT ON CRIMINAL LAW OR FEDERAL CIVIL ENFORCEMENT. Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this Act, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute. Nothing in this section shall be

18

Goldberg, Holding Big Tech Accountable, Dec. 1, 2021

construed to prevent, impair, or limit the enforcement by the United States, or any agency thereof, of any civil Federal statute or regulation.

(2) NO EFFECT ON INTELLECTUAL PROPERTY LAW. Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) STATE LAW. Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought, and no liability may be imposed, under any state or local law that is inconsistent with this section.

(4) NO EFFECT ON COMMUNICATIONS PRIVACY LAW. Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986, or any of the amendments made by such Act, or any similar State law.

(5) NO EFFECT ON SEX TRAFFICKING LAW. Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit—

(A) any claim in a civil action brought under section 1595 of title 18, United States Code, if the conduct underlying the claim constitutes a violation of section 1591 of that title;

(B) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 1591 of title 18, United States Code; or

(C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of title 18, United States Code, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

(6) NO EFFECT ON ANTI-TERRORISM CLAIMS. Nothing in this section shall be construed to prevent, impair, or limit any claim in a civil action brought under section 2333 of title 18, United States Code.

(7) NO EFFECT ON CHILD SEX ABUSE OR CHILD SEXUAL EXPLOITATION CLAIMS. Nothing in this section shall be construed to prevent, impair, or limit any civil action brought under state or federal law relating to claims of child sexual abuse or child sexual exploitation.

(8) NO EFFECT ON CYBER-STALKING LAWS. Nothing in this section (other than 12 subsection (c)(2)(A)) shall be construed to prevent, impair, or limit any civil action in state or federal court relating to harm suffered from conduct that would constitute a violation of section 2261A(2) of title 18, United States Code.

(9) NO EFFECT ON ANTITRUST LAWS. Nothing in this section shall be construed to prevent, impair, or limit any civil action brought under the Federal antitrust laws.

(10) NO EFFECT ON PRODUCT LIABILITY CLAIMS. Nothing in this section shall be construed to prevent, impair, or limit any civil action brought against an Interactive Computer Service for its own defects in its design, manufacture, or failures to warn users and the public of serious risks.

(11) NO EFFECT ON WRONGUL DEATH ACTIONS. – Nothing in this section shall be construed to prevent, impair, or limit any civil action for a wrongful death.

~~(f)~~ (g) DEFINITIONS. As used in this section:

(1) INTERNET.

The term "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) INTERACTIVE COMPUTER SERVICE.

The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) ~~INFORMATION~~ SPEECH CONTENT PROVIDER.

The term "~~information~~ speech content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service. Being responsible in whole or in part for the creation or development of speech includes, but is not limited to, instances in which a person or entity solicits, comments upon, receives payment or payment in-kind for, funds, algorithmically directs, provides testimony under oath as an executives employed by the interactive computer service, or affirmatively and substantively contributes to, modifies, or alters speech provided by another person or entity.

(4) ACCESS SOFTWARE PROVIDER.

The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

20

Goldberg, Holding Big Tech Accountable, Dec. 1, 2021

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

**A.M.**,

Plaintiff,

v.

**OMEGLE.COM, LLC**,

Defendant.

No. 3:21-cv-01674-MO

OPINION AND ORDER

**MOSMAN, J.,**

This case is before me on Defendant Omegle.com LLC's Motion to Dismiss [ECF 17] and Request for Judicial Notice [ECF 18]. At oral argument, I granted in part and denied in part the Motion to Dismiss and granted the Request for Judicial Notice. Mins. of Proceeding [ECF 28]. I write to expound upon some of my oral rulings on the Motion to Dismiss.

**LEGAL STANDARD**

To survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A pleading that offers only "labels and conclusions" or "'naked assertion[s]' devoid of 'further factual enhancement'" will

not suffice. *Id.* (quoting *Twombly*, 550 U.S. at 555, 557). While the plaintiff does not need to make detailed factual allegations at the pleading stage, the allegations must be sufficiently specific to give the defendant fair notice of the claim and the grounds on which it rests. *Erickson v. Pardus*, 551 U.S. 89, 93 (2007) (per curiam) (citing *Twombly*, 550 U.S. at 555).

**BACKGROUND**

Plaintiff, A.M., brings this products liability case against Omegle.com LLC ("Omegle") for connecting (at the time) minor Plaintiff with an adult man who sexually abused her online through Omegle. Compl. [ECF 1] ¶¶ 1–12.

A.M. was eleven years old in 2014 when Omegle, a "free online chat room that randomly pairs strangers from around the world for one-on-one chats," paired her with Ryan Fordyce, a man in his late thirties. *Id*. ¶¶ 2, 7. Over the next three years Fordyce forced A.M. to send pornographic images and videos of herself to him, perform for Fordyce and his friends, and recruit other minors for Fordyce to abuse. *Id*. ¶¶ 8–9. Fordyce threatened A.M. that if she reported him, he would release the videos and pictures and she would get arrested. *Id*. ¶ 10.

Canadian law enforcement raided Fordyce's home in January 2018 and found thousands of files of child pornography on his computer including 220 images and videos of Plaintiff. *Id*. ¶¶ 11, 50. Investigators identified A.M., who by then was fifteen years old, by the high school sweatshirt she wore in photographs she had sent to Fordyce. *Id*. ¶ 50. Fordyce has been criminally charged and is awaiting sentencing. *Id*. ¶ 11.

A.M. brings the following claims in this civil action against Omegle: (1) product liability arising out of defects in design, (2) product liability arising out of defects in warning, (3) negligence in design, (4) negligence in warning and instruction, (5) 18 U.S.C. § 2421A for facilitation of sex trafficking, (6) 18 U.S.C. § 1595 and 18 U.S.C. § 1591 for sex trafficking of

children by force, fraud, or coercion, (7) ORS 30.867 for human trafficking, and (8) negligent misrepresentation. *Id*. ¶¶ 78–152.

**DISCUSSION**

At oral argument I denied Omegle's motion to dismiss claims one through four, I dismissed claim five and seven with prejudice, and I dismissed claims six and eight with leave to amend. Mins. of Proceeding [ECF 28]. I lay out additional reasoning for my decision regarding claims one through seven below.[1]

**I. Section 230 Immunity Does Not Apply to Claims One Through Four**

The threshold matter to be decided is whether Omegle is immune from suit under the immunity provision of the Communications Decency Act ("CDA"), 47 U.S.C. § 230(c)(1) ("Section 230"). Ultimately, I find that Omegle is not immune under Section 230 and DENY Defendant's motion on claims one through four.

Omegle contends that it is entitled to immunity under the CDA, no exceptions to the Act apply, and therefore, Plaintiff's claims are barred. Mot. to Dismiss [ECF 17] at 3. Specifically, Omegle argues Section 230 immunity is warranted because, "[a]t its core, the Complaint alleges that Omegle failed to adequately monitor or police the content or interactions of its users, including by allegedly failing to enforce its user policies and implement safety measures that would have prevented Plaintiff's communication with Fordyce." *Id*. at 5. Omegle goes on to argue that "[n]o matter the labels applied, each of the claims are based on the core premise that Omegle allegedly failed to monitor the interactions of its users and police their content or, stated differently, failed to incorporate adequate protections against the improper content or conduct of its users." *Id*. at 8. Because, Omegle contends, these allegations underlie each of Plaintiff's

[1] I do not discuss claim eight because I granted the motion to dismiss claim eight with leave to amend, but Plaintiff chose not to include this claim in her Amended Complaint [ECF 29] filed after oral argument.

claims, Omegle is entitled to immunity. *Id*. Omegle surmises Plaintiff is merely trying to "shift liability" to it for Fordyce's unlawful actions. *Id*. at 6. Ultimately, so goes the argument, because the failure to monitor that Plaintiff is really alleging is the work of a publisher under Section 230, and publishers are afforded immunity, Omegle argues it should be entitled to immunity. I disagree.

Publisher immunity under Section 230 rests on three prongs. It precludes liability for (1) a provider or user of an interactive computer service (2) whom plaintiff seeks to treat as a publisher or speaker (3) of information provided by another information content provider. *Gonzalez v. Google LLC*, 2 F.4th 871, 891 (9th Cir. 2021) (quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100–01 (9th Cir. 2009)).

**A. Whether Omegle Is a Provider or User of an Interactive Computer Service**

Here, the parties do not disagree on the first prong—whether Omegle is a provider or user of an interactive computer service. The CDA defines an interactive computer service as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server[.]" 47 U.S.C. § 230(f)(2). This definition is expansively interpreted by the Ninth Circuit, with websites identified as the most common interactive computer services. *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1268 (9th Cir. 2016). Omegle is a website and comfortably fits the definition.

**B. Whether Omegle is a Publisher or Speaker of Information**

Omegle argues that it is a publisher of information, namely of the communications between Fordyce and A.M., and therefore, the second prong of the *Gonzalez* test is met.

At the outset, "what matters is not the name of the cause of action … what matters is whether the cause of action inherently requires the court to treat the defendant as the 'publisher

or speaker' of content provided by another." *Barnes*, 570 F.3d at 1101–02. Stated differently, "courts must ask whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a 'publisher or speaker.' If it does, section 230(c)(1) precludes liability.'" *Id*. Publication "involves reviewing, editing, and deciding whether to publish or to withdraw from publication [of] third-party content." *Id*. at 1102.

The most important case for resolving this issue of Section 230 liability is *Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021). In *Lemmon*, the Ninth Circuit reversed a district court's dismissal of a plaintiff's amended complaint on the grounds of Section 230 immunity, allowing plaintiff's negligent design lawsuit to proceed.

The suit in *Lemmon* was brought by the surviving parents of two boys who died in a car crash. The boys in the car were driving at speeds near 123 mph and were going 113 mph when the car left the road, crashed into a tree, and burst into flames. *Id.* at 1088. Shortly before the crash, one of the boys opened the phone application SnapChat to document how fast they were going. *Id.* The parents alleged that the boys were trying to drive over 100 mph because of the "speed" filter that overlayed the speed being traveled on a photograph shared through the application. Many SnapChat users believed that going over 100 mph would earn the user a reward and speeding in excess of 100 mph is a game the users played. *Id.* at 1089

Like the instant case, the parties did not dispute whether the defendant was a provider of an interactive computer service. *Id.*at 1091. The dispositive question was whether the cause of action treated the defendant as the publisher or speaker of third-party content. *Id*. at 1093. The Ninth Circuit concluded it did not because the claims turned on the design of SnapChat. *Id*.

In *Lemmon* the parents alleged that "Snap created: (1) Snapchat; (2) Snapchat's Speed Filter; and (3) an incentive system within Snapchat that encouraged its users to pursue certain

unknown achievements and rewards." *Id*. at 1091. Because the Ninth Circuit found this to be an adequately pled products liability tort that provided a duty to exercise due care, Section 230 immunity did not apply. *Id.* at 1092–93. And because "Snap could have satisfied its alleged obligation—to take reasonable measures to design a product more useful than it was foreseeably dangerous—without altering the content that SnapChat's users generate[,] Snap's alleged duty in this case has nothing to do with its editing, monitoring, or removing of the content that its users generate through Snapchat." *Id*. at 1092 (internal quotation marks and citations omitted).

Here, Plaintiff's complaint adequately pleads a product liability lawsuit as to claims one through four.[2] Omegle could have satisfied its alleged obligation to Plaintiff by designing its product differently—for example, by designing a product so that it did not match minors and adults. Plaintiff is not claiming that Omegle needed to review, edit, or withdraw any third-party content to meet this obligation. As I will discuss in more detail below, the content sent between Plaintiff and Fordyce does not negate this finding or require that I find Omegle act as a publisher.

The Ninth Circuit held in *Lemmon* that a defendant "allow[ing] its users to transmit user-generated content to one another does not detract from the fact that [a plaintiff] seek[s] to hold [the defendant] liable for its role in violating its distinct duty to design a reasonably safe product." 995 F.3d at 1092. "The duty to design a reasonably safe product is fully independent of [a defendant's] role in monitoring or publishing third party content." *Id*. In *Lemmon* it was immaterial that one of the decedents had sent a SnapChat with the speed filter on it. Instead, what mattered is that the claim treated defendant as a product manufacturer by accusing it of

[2] See, for example, Paragraph 80 (which appears to be crafted with *Lemmon* in mind) which reads, "Omegle is defectively designed. Namely, the combination of the website's user anonymity and the absence of age restrictions amount to a design defect. This design defect creates the predictable consequence of attracting both unsuspecting children and predatory adults, thereby facilitating and encouraging dangerous behavior and harm to children using the product." Compl. [ECF 1] ¶80.

negligently designing a product (SnapChat) with a defect (the interplay between the speed filter and the reward system).

In this case, it similarly does not matter that there were ultimately chats, videos, or pictures sent from A.M. to Fordyce. As I stated at oral argument, it is clear that content was created; however, claims one through four do not implicate the publication of content. Tr. [ECF 32] at 10:6–11:8. What matters for purposes of those claims is that the warnings or design of the product at issue led to the interaction between an eleven-year-old girl and a sexual predator in his late thirties.

Omegle argues that this framework would contradict *Doe v. Twitter, Inc.*, 555 F. Supp. 3d 889 (N.D. Cal. Aug. 19, 2021). In *Doe*, plaintiffs brought suit against defendant Twitter alleging that Twitter permits and even aids in the distribution of child pornography and failed to remove pornographic content, including the plaintiffs. *Id*. at 894. There, the district court found the case before it distinguishable from *Lemmon* on Section 230 immunity because:

> [T]he nature of the alleged design flaw in this case—and the harm that is alleged to flow from that flaw—is directly related to the posting of third-party content on Twitter. In particular, Plaintiffs allege that Twitter's design, which is aimed at enabling its users to disseminate information very quickly to large numbers of people through such features as hashtags and algorithms, also enables sex traffickers to distribute CSAM on a massive scale.

*Id*. at 930 (internal quotations omitted). The court went on to find that the publication function was implicated because, "[i]n other words … Twitter would have to alter the content posted by its users" by preventing the posting of third-party content containing child pornography. *Id*.

Omegle failed to demonstrate why, in its briefing or at oral argument, the instant case is more like *Doe* than *Lemmon*. Here, Plaintiff alleges that Omegle is defectively designed, and that Plaintiff fails to warn child users of adult predators on the website. Resp. in Opp'n [ECF 23] at 16. In order to meet the obligation A.M. seeks to impose on Omegle, Omegle would not have to

alter the content posted by its users—it would only have to change its design and warnings. In that way, this case is easily distinguished from *Doe* and analogous to *Lemmon*. Therefore, I find that Plaintiff does not seek to treat Omegle as a publisher of information under Section 230 of the CDA under *Lemmon*.

**C. Whether the Case Turns on Information Provided by Another Information Content Provider**

In *Lemmon*, the Ninth Circuit identified the case as a "clear example of a claim that simply does not rest on third party content." 995 F.3d at 1093. In *Lemmon*, the parents did not fault the Snap for the images it published. Instead, because the parents' claim rested on nothing more than the Snap's "own acts," Snap was not entitled to Section 230 immunity. *Id*. at 1094 (internal quotation marks omitted).

Here, Omegle has attempted to make this a case about Fordyce's communications to the Plaintiff, but as discussed above, Plaintiff's case does not rest on third party content. Plaintiff's contention is that the product is designed a way that connects individuals who should not be connected (minor children and adult men) and that it does so before any content is exchanged between them. Resp. in Opp'n [ECF 23] at 10–11 ("The random pairing function of adults and children and the service's accessibility to both adults and children work in tandem. Plaintiff's claims thus have nothing to do with information provided by a user. It is the website's sole function of randomly matching children with adults that causes the danger. This function occurs before content occurs.")

Because this is a products liability case that does not rest on Defendant's publication of third-party content, I find that Section 230 immunity does not apply and DENY the Motion to Dismiss as to claims one through four.

## II. Claims Five and Seven

At oral argument, I dismissed claims five and seven with prejudice. Mins. of Proceeding [ECF 28]. I write to provide greater detail on my reasoning.

### A. Claim Five: 18 U.S.C. § 2421A Promotion or Facilitation of Prostitution and Reckless Disregard of Sex Trafficking

Defendant argues that this claim is barred because 18 U.S.C. § 2421A does not apply retroactively and supports this assertion with an analysis of the text and structure of the law. Mot. to Dismiss [ECF 17] at 24–28.

Congress enacted 18 U.S.C. § 2421A in April 2018 as a part of the "Allow States and Victims to Fight Online Sex Trafficking Act of 2017" ("FOSTA") Public Law No. 115-164. As I will discuss in more detail in regard to Claim Six, FOSTA abrogated Section 230 immunity for federal sex trafficking claims. Relevant for purposes of claim five, FOSTA enacted a new federal criminal offense and a new civil cause of action allowing the recovery of attorney fees—18 U.S.C. § 2421A.

In Section 4 of FOSTA, the section that abrogates Section 230 immunity, Congress included the following: "(b) Effective Date.—The amendments made by this section shall take effect on the date of the enactment of this Act, and the amendment made by subsection (a) shall apply regardless of whether the conduct alleged occurred, or is alleged to have occurred, before, on, or after such date of enactment." Subsection (a) refers to the language added to Section 230(e) of the CDA—it does not refer to the entirely different section of the legislation that enacted 18 U.S.C. § 2421A. Further, the section enacting 18 U.S.C. § 2421A does not contain a similar provision explicitly stating that this provision of the public law was intended to be applied retroactively. Therefore, the plain text of the statute does not apply 18 U.S.C. § 2421A retroactively.

In this case, the police raided Fordyce's home in January of 2018 and found evidence of his abuse of A.M.. Compl. [ECF 1] ¶ 11, 50. FOSTA became law in April 2018. Pub. Law No. 115-164. Accordingly, I DISMISS claim five with prejudice. Tr. [ECF 32] at 14:11–12.

**B. Claim Seven: Violation of ORS 30.867 (Action for Violation of Criminal Laws Relating to Involuntary Servitude or Trafficking of Persons)**

Omegle argues that although FOSTA created a carveout to Section 230 immunity for certain federal sex trafficking claims, there is no corresponding exclusion for state law civil claims. Mot. to Dismiss [ECF 17] at 23–24. The plain language of 47 U.S.C. § 230(e)(5) supports this interpretation as it does not provide a carveout for civil state trafficking claims. 47 U.S.C. § 230(e)(5) provides carveouts for Section 230 immunity only for the following:

> (A) any claim in a civil action brought under section 1595 of title 18, United States Code, if the conduct underlying the claim constitutes a violation of section 1591 of that title; (B) any charge in a criminal prosecution brought under state law if the conduct underlying the charge would constitute a violation of section 1591 of title 18, United States Code; or (C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of title 18, United States Code…."

The plain text of the statute does not provide a carve out for civil state law trafficking claims. Therefore, I DISMISS claim seven with prejudice.

**III. Claim Six 18: U.S.C. § 1595 Civil Remedy for § 1591 Sex Trafficking of Children or by Force, Fraud, or Coercion**

Claim six raises three areas of inquiry: (1) what is the correct mens rea, and whether (2) venture and (3) profit were adequately pled. Tr. [ECF 32] at 14:13–14, 16:10–11. At oral argument I ruled that Plaintiff's allegations in the complaint on venture and profit were inadequate and would need to be re-pled to adequately reflect the necessary mens rea. Tr. [ECF 32] 20:20–21:1. Accordingly, this section explains what mens rea is necessary for claims brought under § 1595.

Omegle argues that Plaintiff has failed to allege the correct mens rea in the complaint; specifically, that Plaintiff failed to establish Omegle had met the higher actual knowledge standard under 18 U.S.C. § 1591. Therefore, Omegle cannot be held liable under FOSTA because FOSTA only abrogates Section 230 immunity for "any claim in a civil action brought under section 1595 of Title 18, if the conduct underlying the claim constitutes a violation of section 1591 of that title." 47 U.S.C. § 230(e)(5)(A).

As I explained at oral argument, "you can sue under Section 1595 and not run afoul of Section 230 immunity 'if the conduct underlying the claim constitutes a violation of Section 1591.'" Tr. [ECF 32] at 14:18–20 (citing 47 U.S.C. § 230(e)(5)(A)). A civil claim brought under § 1595 is predicated on the violation of § 1591. And § 1595 and § 1591 have different mens rea standards: § 1595 has a "knew or should have known" mental state and § 1591 contains an actual knowledge mental state.

This argument presents a question of statutory interpretation that is playing out in district courts throughout the Ninth Circuit: Did Congress intend to only waive Section 230 immunity for civil claims under § 1595 that are predicated on a violation of § 1591?

Defendant argues in its motion that the complaint does not state a plausible claim for violation of § 1591 because it does not use the correct mens rea and therefore, an exception to Section 230 immunity under Section230(e)(5)(A) does not apply. Mot. to Dismiss [ECF 17] at 14–23. Omegle relies on the court's reasoning in *J.B. v. G6 Hospitality, LLC*, No. 19-cv-07848-HSG, 2021 WL 4079207, at *18 (N.D. Cal. Sept. 8, 2021), where the Court found the § 1591 mens rea applied. Plaintiff instead posits that Section 230 immunity "does not affect sex trafficking laws." Resp. in Opp'n [ECF 23] at 24. Plaintiff directs me to *Doe v. Twitter*, in which

the Northern District of California found the plaintiff only had to allege the less stringent mens rea of "knew or should have known." 555 F. Supp. 3d at 918.

Here, I agree with the approach from *J.B.* and find that text of Section 230(e)(5)(A), on its face, imports the higher mens rea from § 1591 into § 1595. Like the court in *J.B.*, I too find that the "most straightforward reading to be that the provision provides an exemption from CDA immunity for a section 1595 claim if the civil defendant's conduct amounts to a violation of section 1591." *J.B.*, 2021 U.S. Dist. LEXIS 170338, at *18 (citing *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997)).

As I stated at oral argument, the court in *Doe* employs a different statutory analysis by first looking at the statutory text but disagreeing with the outcome because it is in some way nonsensical. Tr. [ECF 32] 15:24–16:2. Specifically, the *Doe* court found that "the implication of this reading is that a sex trafficking victim who seeks to impose civil liability on an ICS provider on the basis of beneficiary liability faces a higher burden than a victim of sex trafficking who seeks to impose such liability on other types of defendants." 555 F. Supp. 3d at 920. For that reason, the *Doe* court rejects importing the higher mens rea of Section 1591 into Section 1595.

This issue is far from settled in the Ninth Circuit. Both *Doe* and *J.B.* have been appealed. *Doe*, 555 F. Supp. 3d 889, *appeal docketed*, No. 22-15104 (9th Cir. Jan. 25, 2022); *J.B.*, No. 19-cv-07848-HSG, 2021 U.S. Dist. LEXIS 170338 (N.D. Cal. Sept. 8, 2021), *interlocutory appeal granted*, No. 21-80133 (9th Cir. Feb. 28, 2022).

Because I agree with the *J.B.* court's statutory interpretation, I GRANT Defendant's motion to dismiss claim seven, but do so without prejudice.

**CONCLUSION**

For the reasons discussed above and on the record at oral argument on May 9, 2022, I GRANT in part and DENY in part Defendant's Motion to Dismiss [ECF 17] and I GRANT Defendant's Request for Judicial Notice [ECF 18].

IT IS SO ORDERED.

DATED this 13 day of July, 2022.

Michael W. Mosman
MICHAEL W. MOSMAN
Senior United States District Judge

Barbara C. Long, OSB No. 122428
barb@vogtlong.com
VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
Telephone: (503) 228-9858

Carrie Goldberg (*pro hac vice*)
carrie@cagoldberglaw.com
Naomi Leeds (*pro hac vice*)
naomi@cagoldberglaw.com
C.A. GOLDBERG PLLC
16 Court Street 33rd Floor
Brooklyn, NY 11241
Telephone: (646) 666-8908

*Attorneys for Plaintiff*

**UNITED STATES DISTRICT COURT**

**FOR THE DISTRICT OF OREGON**

**PORTLAND DIVISION**

| | |
|---|---|
| A.M., an individual,<br><br>Plaintiff,<br><br>v.<br><br>OMEGLE.COM LLC,<br><br>Defendant. | Case No. 3:21-cv-01674-MO<br><br>**SECOND AMENDED COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

PLAINTIFF, by and through her attorneys of record, and for her Second Amended Complaint against Defendant, alleges as follows:

**PRELIMINARY STATEMENT**

1. This is a product liability case against a company that profits from procuring children for sexual predators.

2. Omegle is a free online chat room that randomly pairs strangers from around the world for one-on-one video chats, inviting users to "Talk to Strangers!"

3. As soon as two people are matched, they are immediately face-to-face with a stranger on their screens.

4. Omegle markets its product to children as young as 13 and knowingly matches its child users with adults.

5. Omegle's most regular and popular use is for live sexual activity, such as online masturbation. Omegle employs no mechanism to verify ages to prevent children from being matched with adults. Children cannot opt out of matching with adults. Nor can adults opt out of matching with children.

6. Omegle is aware that users engage in sexual and masturbatory conduct on their platform. On its homepage, Omegle flouts the dangers of its product, acknowledging that Omegle users "may not behave appropriately" and that their moderation "is not perfect" enough to ban "misbehaving users."

7. In approximately 2014, Omegle paired then eleven-year-old A.M. with Ryan Scott Fordyce ("Omegle Predator") who was in his late thirties at the time.

8. Over the next three years, the Omegle Predator forced A.M. to take and send naked photos and videos of herself engaging in sex acts of his choosing. He coerced A.M. to record herself masturbating with her hands and objects, urinating, and engaging in other



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

sexual acts. Sometimes he made A.M. perform for him and his friends.

9. The Omegle Predator also dispatched A.M. back onto Omegle to recruit other kids for him to abuse.

10. The Omegle Predator regularly threatened A.M. that if she reported to police or told anybody about their activities, he would share his trove of pictures and videos and that she would get arrested.

11. In January 2018, the Omegle Predator's home was raided by law enforcement, and 3,055 files of child pornography were found on his devices, including 220 images and videos of A.M. He currently awaits sentencing.

12. Plaintiff seeks recovery against Omegle on her claims for:

a. Product liability arising out of defects in design and defects in warning;

b. Negligence in design, warning, and instruction; and

c. 18 U.S.C. § 1595.

**PARTIES, JURISDICTION, AND VENUE**

13. Plaintiff A.M. is an American citizen currently residing in Christchurch, New Zealand. She was born in 2002 and at all times relevant to this action was a minor. Plaintiff wishes to proceed via the use of a pseudonym because of the sensitive and highly personal nature of the case, which involves allegations of a sexual nature for events that occurred while Plaintiff was a minor.

14. Defendant Omegle.com LLC ("Omegle") is a Limited Liability Company organized in the State of Oregon with its principal place of business in Florida.

15. Venue is proper under 28 U.S.C. § 1391(a) because Defendant resides in



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

Multnomah County, Oregon.

16. Subject matter jurisdiction is proper under 28 U.S.C. § 1332 because the amount in controversy is over $75,000.00 and there is complete diversity of the parties.

**FACTS**

**Omegle's Product Design**

17. Omegle is a free online website that randomly pairs users so they can livestream video chat with a stranger.

18. Originally launched in 2009, Omegle is one of the largest and most popular chat sites with users from countries all over the world and about 66,000,000 monthly visits. At any given time, there are typically around 50,000 users online ready to chat.

19. Leif K-Brooks founded Omegle and remains CEO today.

20. According to data published by BBC, Omegle usage doubled during the pandemic between January 2020 and January 2021.

21. Omegle's innovation to the world of chatting apps is its complete user anonymity, designed to make connections quick, convenient, and discreet. The random users are identified as "You" and "Stranger."

22. Omegle's anonymized stranger-matching is integral to its business model encouraging its users to "Talk to strangers!"



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858


23. Omegle is designed for users to cycle quickly through strangers. As soon as users tire of a stranger Omegle connects them with, they can click a "stop" button and be transported to the screen of a different user, who likewise appears in their screen.

24. Omegle is often used for individuals seeking an immediate online sexual connection with a stranger.

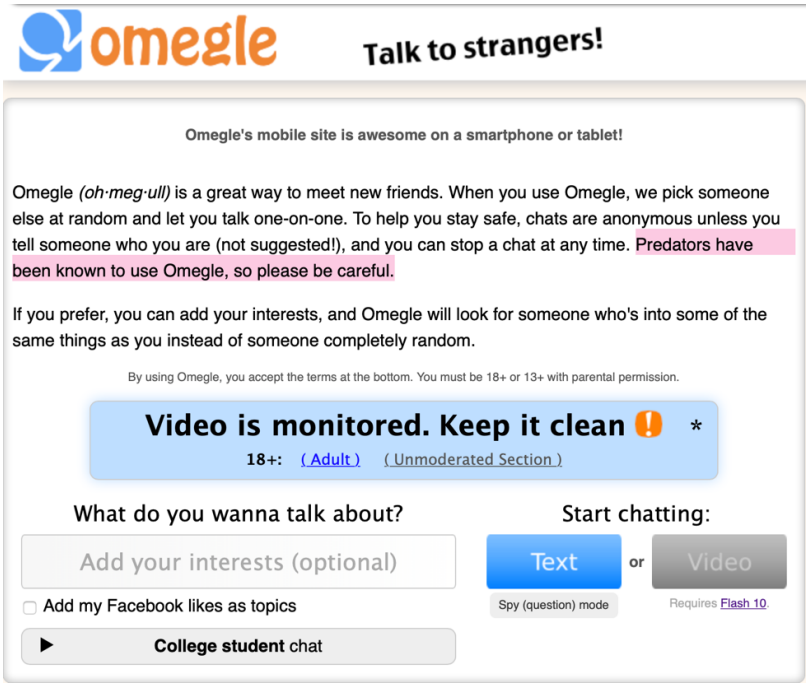
25. Within seconds of using Omegle, users are likely to come face-to-face with nude users whether they want to or not.



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

26. Omegle acknowledges that its product is home to predators but puts the onus on its users to not be preyed upon. Up through May 2021, its homepage read "Predators have been known to use Omegle, so please be careful."



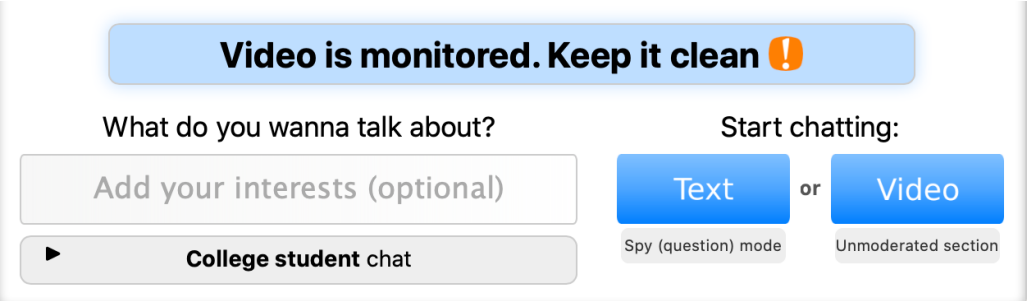

27. Omegle allows anybody to use its product and requires no registration, name, or age verification. Nor does it require users to register using other industry-standard verifiers such as an email, phone number, or social media account.

28. Omegle's content moderation practices are reckless to the point of being altogether absent. Omegle's homepage provides that "Omegle video chat is moderated but no moderation is perfect." It provides in large lettering toward the bottom of the page: "Video is monitored. Keep it clean!" Despite its claim of not "perfect" moderation, the site also confusingly labels its Video chat button as the "Unmoderated section."



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858




29. Omegle knows kids use its product and allows kids as young as 13 to do so despite there being an extraordinarily high probability that within just a couple matches, a child is likely to be face to face with a masturbating adult. The sole warning for kids on Omegle's website states "[y]ou must be 18+ or 13+ with parental permission and supervision to use Omegle." Omegle does not actually require children to state their age or birth date to register for the product or confirm they have parental permission. The parental permission is legally deficient because parents cannot provide legal authorization for their children to become crime victims.

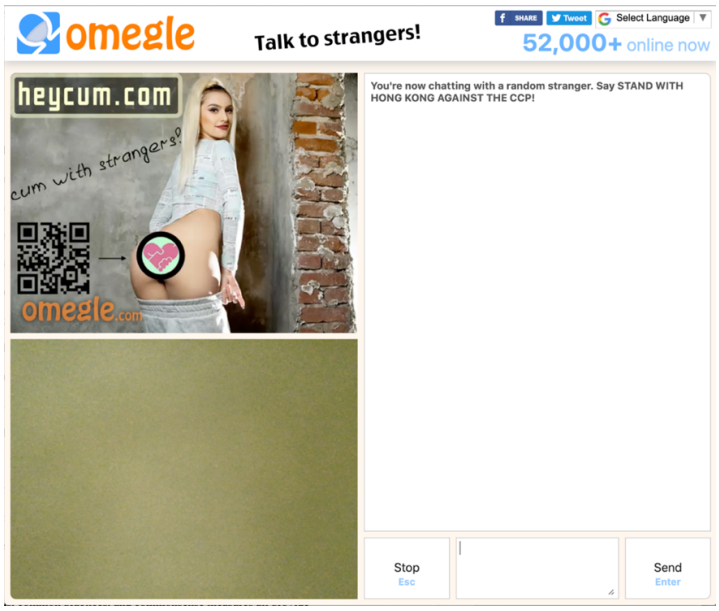
30. Unlike many other internet products, Omegle is accessible only through its own website. In contrast, applications uploaded through a marketplace like the App Store or Google Play, where consumers are verified, provide an additional check and balance to prevent abuse.

31. Omegle's revenue model appears to derive from selling user and usage data and by selling advertisements on its website. The advertisements are generally for pornographic and adult web cam sites. For example, below is a screenshot of an Omegle.com screen on July 7, 2021, that offers users the chance to "cum with strangers!"



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858




32. Ads for websites like heycum.com would be visible even to these 13-year-olds that Omegle says can use its product with parental permission.

33. In February of 2021, BBC published an article detailing the prevalence of child sexual abuse material and grooming on Omegle. During the approximately 10 hours BBC journalists monitored Omegle, they reported being paired with dozens of minors, some appearing as young as seven or eight. Twice the journalists were paired with young prepubescent boys masturbating. In just one two-hour period, the BBC was connected at random with 12 masturbating men, eight naked males, and seven pornography advertisements. Joe Tidy, "Omegle: Children expose themselves on video chat site," BBC NEWS, (February 18, 2021), https://www.bbc.com/news/technology-56085499, (last visited October 24, 2021).



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

34. According to the BBC, in the past couple of years, schools, police forces, and government agencies have issued warnings about Omegle in the US, UK, Norway, France, Canada, and Australia.

35. At all relevant times, Omegle represented to users in its privacy and community standards page that it protects users and values the web site's "safety, security and integrity."

36. At all relevant times, Omegle represented its ability to ban or deny access to offending or unauthorized accounts in its Terms and Conditions of Service ("Terms of Service") dated July 1, 2014 (Wayback Machine, http://web.archive.org/web/20140701135308/http://www.omegle.com/. These Terms of Service provide in relevant part:

a. By using the Omegle Web site, and/or related products and/or services ("**Omegle**", provided by Omegle.com LLC), **you agree to the following terms**: Do not use Omegle if you are under 13. If you are under 18, use it only with a parent/guardian's permission. Do not transmit nudity, sexually harass anyone, publicize other peoples' private information, make statements that defame or libel anyone, violate intellectual property rights, or behave in any other inappropriate or illegal way on Omegle. Understand that human behavior is fundamentally uncontrollable, that the people you encounter on Omegle may not behave appropriately, and that they are solely responsible for their own behavior. Use Omegle at your own peril. Disconnect if anyone makes you feel uncomfortable. You may be denied access to Omegle for inappropriate



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

behavior, or for any other reason. OMEGLE IS PROVIDED AS IS, AND TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW, IT IS PROVIDED WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, NOT EVEN A WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW, THE PROVIDER OF OMEGLE, AND ANY OTHER PERSON OR ENTITY ASSOCIATED WITH OMEGLE'S OPERATION, SHALL NOT BE HELD LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES ARISING FROM THE USE OF OMEGLE, OR ANY OTHER DAMAGES RELATED TO OMEGLE OF ANY KIND WHATSOEVER. By using Omegle, you accept the practices outlined in Omegle's PRIVACY POLICY and INFORMATION ABOUT THE USE OF COOKIES (updated 2014-06-03 – contains important information about video chat monitoring).

b. Parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist you in limiting access to material that is harmful to minors. If you are interested in learning more about these protections, information is available at http://kids.getnetwise.org/tools/as well as a number of other Internet sites that provide information on this form of protection.

c. * Omegle video chat is moderated. However, moderation is not perfect. You may still encounter people who misbehave. They are solely responsible for their own behavior.



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

37. Although it sometimes represents that it will take a hard line against anyone who uses Omegle in abusive ways, Omegle does not actually do so. Just in the last year, Omegle has continued to be the subject of warnings from cybercrime experts and law enforcement officers all over the world. Omegle has taken no known action to mitigate the threat of child exploitation on Omegle. The failures of Omegle have been reported in numerous media outlets. (E.g., Christel Bell, "Cyber crime experts warn of Omegle chat site, growing in popularity with kids – and predators," FOX4 (November 10, 2020), https://fox4kc.com/news/cyber-crime-experts-warn-of-omegle-chat-site-growing-in-popularity-with-kids-and-predators/, (last visited July 7, 2021); Ashley Franklin, "Police warn Lincolnshire parents about website popular with children," LINCOLNSHIRE LIVE, (April 22, 2021), https://www.lincolnshirelive.co.uk/news/local-news/police-warn-lincolnshire-parents-website-5329461, (last visited July 7, 2021); Olivia Gantzer, "Thames Valley Police warning about new app, Omegle," BRACKNELL NEWS (June 7, 2021), https://www.bracknellnews.co.uk/news/18501651.thames-valley-police-warning-new-app-omegle/, (last visited July 7, 2021).)

38. Upon information and belief, Omegle's owners and operators make little to no effort to screen and monitor the activities of its members or to implement a report function that can flag abusive users. However, they are aware of the dangerous uses of their product given the recently removed warning stating: "Predators have been known to use Omegle, so please be careful." Omegle does not utilize proven and common software that would allow it to identify and block abusive users or identify and deny access to minors.

**Omegle matches a Predator to Plaintiff**



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

39. In or about 2014, the Omegle Predator logged onto Omegle and was paired via text chat with A.M., an 11-year-old girl living with her family in Michigan. This was A.M.'s first time using Omegle alone. Other times, she and her friends had used it to have age-appropriate video chats at sleepovers.

40. On the Omegle platform, the Omegle Predator asked A.M. her age to which she responded, "Eleven." The Omegle Predator continued the conversation and convinced A.M. that it was okay for them to keep communicating.

41. By the end of this 15-minute chat, A.M. found herself believing the Omegle Predator and trusting that he would help her "feel better"—something he had promised her.

42. The Omegle Predator asked A.M. for her contact information so they could stay in touch after the video chat ended.

43. That same night, the Omegle Predator strategically gained A.M.'s trust and induced A.M. to send him photos of herself. First of her smile, and eventually, of her breasts, vagina, and other parts of her body. The Omegle Predator convinced A.M. that it was integral to her "healing" to trust him even if she felt uncomfortable.

44. Within the first two weeks of their relationship, the Omegle Predator had groomed A.M. to become dependent on their communications. The Omegle Predator responded to A.M.'s reticence about sending him images by telling her she could stop at any time, but if she did, the images she had already sent would get leaked. He told her that if this happened, she would get in trouble with her family, school, and the police.

45. A.M. feared that if she reported the man she had met on Omegle, she would go to jail. Not to mention the fact she never knew his full name.



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

46. Over time, the Omegle Predator's abuse increased. He demanded A.M. include her face in all pictures and set deadlines for her to meet his demands for what poses, props, positions, and hairstyles he wanted in the pictures. At all hours of the day and night, she was required to be at his beck and call. Always, he threatened to disseminate the content to her family and friends who he said would disown her. Sometimes he threatened to kidnap A.M. or harm her family.

47. As A.M. continued complying, the abuse became more severe, intricate, and sadistic. About 18 months in, the Omegle Predator forced A.M. to join him on group chats and watch him sell, trade, and otherwise traffic her pictures to his fellow pedophiles.

48. Omegle continued to factor heavily into the abuse. The Omegle Predator forced A.M. into sex trafficking other children for him on Omegle. The Omegle Predator trained A.M. to go onto Omegle to recruit other children for him to exploit. On certain days of the week, he would assign Plaintiff to go back onto Omegle for a set number of hours and find other girls who "[he] would like." A.M.'s task would be to take screenshots of them, get their contact information, and relay everything to Fordyce.

49. The abuse and trafficking continued for A.M. between the ages of eleven and fifteen. During these years the former A-student was frequently absent from school and withdrawn from friends and family.

50. On January 12, 2018, when A.M. was 15, her parents were contacted by Canadian law enforcers who had identified her based on the high school sweatshirt she was wearing in a picture they saw of her. The Canadian law enforcers said they had raided the



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

home of a man name Ryan Fordyce and recovered 3,055 files of child pornography across his devices, including 220 images and videos of A.M.

51. The Omegle Predator has pled guilty to possession of child pornography for the purpose of distribution or making available child pornography and communication with a person who is, or believed to be, under the age of 18 years old by means of telecommunication. In so doing, he admitted to meeting Plaintiff via Omegle when she was a minor, chatting with her on Omegle over a period of several years, possessing numerous graphic images of her in a state of nudity and performing sexual acts, and threatening to report Plaintiff to the police if she told anyone about their conversations.

52. A.M. suffered and continues to suffer serious emotional pain and psychological distress as a result of Omegle's role first in facilitating her first encounter with a predator who abused her for roughly three years and then becoming the stomping grounds where she was forced to recruit more innocent victims for her abuser.

53. Before this, A.M. was a young child developing in a healthy and gratifying way. She loved school and was a skilled horseback rider. After school and over the summers she used to make money working at her parents' ice cream shop scooping ice cream for her friends. All these childhood pleasures vanished because of one night on Omegle. A.M. stopped interacting with friends and doing things that once made her happy because she felt she did not deserve good things. She felt disgusted by her own face and body because she was convinced that all of this was her fault for going on Omegle that one night.

54. A.M. has symptoms of Post-Traumatic Stress Disorder, has suffered seizures, and has panic attacks that render her bedridden for several days to follow.



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

55. A.M. is triggered by certain words and sounds. To this day, she cannot hear the phone ring without having trouble breathing and possibly experiencing a panic attack because of the phone call from law enforcement notifying her parents of the Omegle Predator. For example, A.M. can no longer wear her hair to one side because this was the Omegle Predator's preference when he gave her assignments.

56. A.M. moved far away from Michigan in part because it was so unbearable to live near the darkness and fear from her adolescent and early teen years.

57. A.M. is subject to fear and anxiety when she meets new people. She is in a constant state of hyper-vigilance, fearing that she might be triggered or, worse, develop a relationship with someone who will try to control her.

58. A.M.'s relationship with her mother became incredibly strained as a result of her mother's secondary traumatic stress that has resulted from learning of her daughter's sexual exploitation by the Omegle Predator.

59. The most difficult realization A.M. has had to come to terms with is that every person she becomes close with in the future will eventually learn of the abuse she suffered as a child. No amount of money spent, therapy, or time can erase the trauma or the abuse itself. Plaintiff feels that her future has become as tainted as her past.

60. As a result of her trauma, A.M. sees her past in three compartments of time. The life she lived before the day she logged onto Omegle and met the Omegle Predator, the hell she experienced as his victim, and her current existence which is a struggle every day.



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

61. Plaintiff is now in her second year of college where she is studying psychology in hopes of becoming a professional in children's mental health. She is currently volunteering with youth mental health organizations near her university.

62. Plaintiff is dedicated to forming connections with the children and teenagers in her life to make sure that they know they can get help if they ever need it, and that they should never fear getting into trouble when asking for help. She is working tirelessly to become the ally that her eleven-year-old self was searching for that night on Omegle.

**PLAINTIFF'S HARM WAS THE PREDICTABLE CONSEQUENCE OF OMEGLE'S NEGLIGENT DESIGN AND MANUFACTURE**

63. Omegle knew or should have known that predators use its product to groom and exploit children sexually. By failing to take action to prevent predators from carrying out these crimes against helpless children on Omegle and failing to cure its negligent design and manufacture, these predatory users felt empowered and incentivized to continue their abusive and malicious use of the product.

64. Prior to 2014 when the Omegle Predator targeted Plaintiff, a series of news articles had been published to warn the public about the dangers of Omegle specific to child exploitation and abuse. E.g., Natasha Chen, "Parents Find Out Daughters Are Targeted Through Online Chat Site," NEWS CHANNEL 3 (October 18, 2012), https://www.wreg.com/news/parents-find-out-daughters-are-targeted-through-online-chat-site/, (last visited November 9, 2021); Brigida Mack, "Mom calls chat website a 'pedophile's paradise'," WBTV (July 16, 2011), https://www.wbtv.com/story/15091703/webiste-a-pedophiles-paradise/, (last visited November 9, 2021); "OK Mother Says Teen Was Sexually Assaulted By Man She Met Online," NEWS9 (October 21, 2013),


C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

https://www.news9.com/story/5e35a7af83eff40362be743b/ok-mother-says-teen-was-sexually-assaulted-by-man-she-met-online, (last visited November 9, 2021).

65. Between May of 2015 and May of 2021, the text on Omegle's homepage included a sentence that read: "Predators have been known to use Omegle, so please be careful." Instead of serving as a warning, though, the statement is an admission that Omegle was well aware that crimes to children were occurring on its platform.

66. Omegle's users, which they allow to be as young as thirteen, but in reality, are often as young as Plaintiff when she was eleven years old, or even younger, have no cognitive or judgment ability to evaluate the warnings or make informed decisions to consent to them.

67. The warning further demonstrates that Omegle authorizes the use of its product in an abusive manner.

68. Despite years of child abuse and exploitation facilitated by Omegle, nothing has been done to remove or restrict child access or to otherwise address the danger Omegle created.

69. In fact, the most recent change to the Omegle homepage occurred in June of 2021, shortly after Plaintiff's counsel sent a preservation letter to Omegle on April 9, 2021, when the sentence, "Predators have been known to use Omegle, so please be careful," was removed.

70. Between its inception and today, Omegle's negligent design and manufacture have created predictable consequences in a way that encourages dangerous behavior. No reasonable measures have been taken to ensure that the product's design is more useful than it is foreseeably dangerous.



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

71. Omegle's product is designed perfectly to be used the way Fordyce used it – to procure children anonymously and without a trace.

72. Omegle failed to take a number of ameliorative actions such as: identifying and banning predatory users through the language detected in chats or its video monitoring function it purports to employ, using common software that could be used to flag specific phrases used repeatedly by offenders, enabling users to report offending users by including a "Report" or "Abusive Content" button on the chat screen, changing its policy to only allow adults 18 and older to use the website, integrating an effective age verification mechanism to ensure that minors are not using the unmonitored video section of the site, requiring users to register their name or phone number with the site so that user misconduct can be traced by the site's administrators, making its product available through third party marketplaces like Apple and Google where customers are verified and downloads are recorded, and/or staffing a community standards and safety department with human beings.

73. Industry standards, common practices, and common-sense measures all provide methods by which Omegle could mitigate the unsafe design of its software.

74. Per its updated Privacy Policy, Omegle collects the very data that it would need to stop the abuse, including but not limited to mobile device identifiers, chat files, image files, location data, browser type, operating system information, IP addresses, cookies, and language data.

**DAMAGES**

75. As a result of Defendant's wrongful conduct, Plaintiff was sexually exploited by Fordyce, and suffered in the past and will suffer in the future, physical and psychological



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

injuries consisting of depression, anxiety, post-traumatic stress disorder, sleep and eating disturbances, shame, lack of trust, issues with sexuality, and difficulty with intimate relationships. All of these injuries have caused and will cause Plaintiff non-economic damages in the approximate amount of $22,000,000.00, the exact amount of which to be determined by a jury at trial.

76. Defendant acted with an outrageous indifference to a highly unreasonable risk of harm and with a conscious indifference to the health, safety, and welfare of others, including Plaintiff. Therefore, Plaintiff is entitled to punitive damages against Defendant in an amount to be determined by a jury at trial.

**FIRST CLAIM FOR RELIEF**

**Product Liability – Defect in design**

77. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint, including paragraphs 21-49, 52-59, 63-76.

78. Omegle designed, coded, engineered, manufactured, produced, assembled, and placed the product, Omegle, in the stream of commerce.

79. Omegle is defectively designed. Namely, the combination of the website's user anonymity and the absence of age restrictions amount to a design defect. This design defect creates the predictable consequence of attracting both unsuspecting children and predatory adults, thereby facilitating and encouraging dangerous behavior and harm to children using the product.

80. Omegle's defective design encourages sexual interactions among people of all ages and by having no age restrictions, it creates a high probability that children will be



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

matched with predatory adults and violated by either exposing themselves or witnessing adults exposing their genitals.

81. Omegle's defective design and regular usage makes breaking the law inevitable – underage users are statistically likely to be matched with nude adults and pedophiles. And adult users, whether clothed or not are statistically likely to be matched with nude children.

82. Omegle's defective design is hospitable to child predators making it foreseeable that the product will be used by predators for immediate sexual moments or to lure children into abusive relationships as happened to A.M. Omegle is therefore a launchpad for predators to target the children they then continue to abuse.

83. Omegle's defective design renders the product unreasonably dangerous.

84. As a direct and proximate cause of Defendant's design, coding, engineering, manufacture, testing, inspection, production, assembly, and sale, Plaintiff sustained permanent injuries and suffered extreme pain and agony.

**SECOND CLAIM FOR RELIEF**

**Product Liability – Defect in Warning**

85. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint, including paragraphs 21-49, 52-59, 63-76.

86. Omegle designed, coded, engineered, manufactured, produced, assembled, and placed the website in the stream of commerce. Omegle contains a defective condition in that use of the website should be permitted only to users 18 and older. Omegle should properly


C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

warn users to notify them that children are strictly prohibited. Instead, Omegle specifically permits children 13 and older to use the product and features an ineffectual and lighthearted warning that understates the risk of using the website as a child.

87. Additionally, Omegle fails to warn its users that there are no remedies to be sought when one witnesses a user who misuses the website. Omegle fails to warn its users that its operators do not and will not take action to ban abusive users.

88. The warning defect makes Omegle unreasonably dangerous.

89. Omegle was designed and manufactured by Defendant and has not been changed and was in the same condition at the time of the injury.

90. As a direct and proximate cause of Defendant's design, coding, engineering, manufacture, production, assembly, and sale, Plaintiff sustained permanent injuries and suffered extreme pain and agony.

**THIRD CLAIM FOR RELIEF**

**Negligent Design**

91. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint, including paragraphs 19-49, 52-59, 63-76.

92. Omegle designed, coded, engineered, manufactured, produced, assembled, and placed the Omegle website in the stream of commerce despite its defective design. Omegle owed a duty to Plaintiff to design the website in such a way that made it safe for its intended use.

93. Omegle knew or should have known when producing the website that it was designed defectively, creating an unreasonable risk of injury to its users, including Plaintiff.



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

94. Omegle designed, coded, engineered, manufactured, produced, assembled, and placed the Omegle server-side software in the stream of commerce. Omegle owed a duty to Plaintiff to design the server-side software in such a way that made it safe for its intended use.

95. Omegle knew or should have known when producing the server-side software that it was designed defectively, creating an unreasonable risk of injury to its users, including Plaintiff.

96. Omegle was negligent in failing to properly design, manufacture, and communicate the defect in the website and server-side software to Plaintiff and other users, creating a clear and immediate risk of serious injury to users such as Plaintiff. As a direct and proximate result, Plaintiff sustained permanent injuries and suffered extreme pain and agony.

**FOURTH CLAIM FOR RELIEF**

**Negligence – Failure to Warn or to Provide Adequate Instruction**

97. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint including paragraphs 21-49, 52-59, 63-76.

98. Omegle owed a duty to Plaintiff to only place in the stream of commerce a product containing adequate warning and instruction. Without such warning or instruction, the product is unreasonably dangerous.

99. The product was placed into the stream of commerce by Omegle and was used by Plaintiff and others in a defective and unreasonably dangerous condition in that it should have contained or been accompanied by warning that the website permits only adults 18 and older. Omegle also failed to warn users that there is no method to report abusive users or to seek relief in the event that one witnesses misuse of the product by another user.



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

100. As a direct and proximate cause of Defendant's negligent failure to provide adequate instruction and warning, Plaintiff sustained permanent injuries and suffered extreme pain and agony.

**FIFTH CLAIM FOR RELIEF**

**18 U.S.C. § 1595 Civil Remedy for § 1591 Sex Trafficking of Children or by Force, Fraud, or Coercion**

101. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint including paragraphs 21-26, 29, 31, 33, 39-50, 51-58, and 79-82.

102. Omegle knowingly, in or affecting interstate or foreign commerce, recruits, entices, harbors, advertises, maintains, patronizes, and solicits persons under the age of 18 knowing and causing them to be used in commercial sex acts.

103. Omegle knowingly benefits, financially and by increasing traffic to their site, from participation in a venture which recruits, entices, harbors, advertises, maintains, patronizes, and solicits persons under the age of 18 knowing and causing them to be used in commercial sex acts.

104. Omegle knowingly introduces children to predators causing children to be victims of sex acts in violation of § 1591.

105. Omegle allows both children and adults to use its product that randomly matches users and encourages users to "Talk to strangers!"

106. Omegle, on its homepage, posted then removed the following phrase: "Predators have been known to use Omegle . . . "



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

107. Upon information and belief, Omegle knew that predators frequented the website for the purpose of meeting children and engaging in child sexual exploitation. Upon information and belief, Omegle knew that children were using the website and being matched with predators. In light of this known risk, Omegle's active solicitation of predators and children constitutes active and knowing participation in the sex trafficking of children.

108. Beginning at the age of 11, Plaintiff was forced to perform commercial sex activities for Fordyce. This continued for about three years during which Fordyce abused Plaintiff and threatened abuse of law or legal process. Plaintiff feared arrest if she stopped performing for him or told anybody.

109. For about three years, Plaintiff was trafficked as a result of the abuse that started on Omegle. Today, Plaintiff continues to be trafficked. Pornographic images and videos depicting her as a child continue to circulate online among predators.

110. Plaintiff suffers extreme harms as a result of Defendant's conduct.

111. Pursuant to 18 U.S.C. § 2421 A(c), Plaintiff seeks compensatory and actual damages and reasonable attorney's fees.

**SIXTH CLAIM FOR RELIEF**

**Negligence**

112. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint including paragraphs 17-76.

113. In the alternative to Claims 1-5 above and pursuant to FRCP 8(d), where Omegle is not considered a "product" under Oregon law.

114. Omegle failed to exercise reasonable care to provide a reasonably safe service.



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

115. Omegle failed to take reasonable measures to provide users with a service more useful than foreseeably dangerous.

116. Omegle created a system that assisted or aided in child sexual exploitation, including the exploitation of Plaintiff by supplying an anonymous and sexual communication platform to children while it knew or had reason to know adult predators were likely to use the platform to target children.

117. Omegle unreasonably created a foreseeable risk of harm that its platform would injure Plaintiff and was negligent.

118. Omegle matches children with adult predators.

119. Omegle is accessible and advertised to both adults and children.

120. The random pairing function of adults and children and the service's accessibility to both adults and children work in tandem.

121. Omegle could have satisfied its obligation to Plaintiff by providing a service that did not match minors and adults.

122. Omegle's matching of adults and children was a substantial contributing causal factor to the abuse of Plaintiff.

123. Plaintiff has a legally protected interest in being free from sexual exploitation and trafficking.

124. Plaintiff's damages include sexual and emotional distress and physical harm.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for a judgment in her favor as follows:



C.A. GOLDBERG, PLLC
16 Court Street
Brooklyn, NY 11241
(646) 666-8908

VOGT & LONG PC
1314 NW Irving St, Suite 207
Portland, OR 97209
(503) 228-9858

1. If successful on any of Plaintiff's claims for relief, non-economic damages in the amount of $22,000,000.00, the exact amount to be determined by the jury;
2. On Plaintiff's Fifth Claim for Relief, awarding Plaintiff her reasonable attorney's fees and costs;
3. If successful on any of Plaintiff's claims for relief, punitive damages for Plaintiff in an amount to be determined by the jury;
4. On All Claims for Relief, awarding plaintiff pre-judgment interest on all damages at the highest rate allowed by law;
5. For Plaintiff's disbursements and incurred costs; and
6. On All Claims for Relief, granting such other and further relief as the Court deems just and equitable.

**PLAINTIFF'S REQUEST FOR A JURY TRIAL**

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a jury trial in this action on all issues triable by a jury.

Dated: August 1, 2022

Respectfully submitted,

*/s/ Barbara Long*
Barbara Long, OSB #122428
Vogt & Long PC
1314 NW Irving St, Suite 207
Portland, Oregon 97209
Tel: (503) 228-9858
Fax: (503) 228-9860
Barb@vogtlong.com

*/s/Carrie Goldberg*
Carrie Goldberg
(*pro hac vice*)

Naomi Leeds
(*pro hac vice*)

C.A. Goldberg, PLLC
16 Court Street, 33rd Fl.
Brooklyn, NY 11241
Tel: (646) 666-8908
Fax: (718) 514-7436
carrie@cagoldberglaw.com
naomi@cagoldberglaw.com

*Attorneys for Plaintiff A. M.*

# Chapter 2

# Presentation Slides: Challenges to Building Trust in AI/ML?

**Caryn Lusinchi**
BiasInAI.com
Portland, Oregon

# Challenges to Building Trust in AI/ML?

**An Exploration into Machine Learning, Data Bias and Model Explainability**

## Caryn Lusinchi

### FCHA, AI Auditor

- IAAIS (Independent Audit of AI Systems)
- GDPR EU and UK
- NYC Bias Law

15+ years in scaling enterprise GTM B-to-B and B-to-C technology at Google, Meta, startups and more.

Founder of www.biasinai.com

Currently, work for Arthur, a Series B software company monitoring data accuracy, bias, fairness and explainability for machine learning models in production.

Connect with me on LinkedIn

# Agenda

**AI OVERVIEW**

AI vs. ML vs. Deep Learning

Applications of ML & Deep Learning

Machine Learning Wofklows & User Experiences

Training Machine Learning Systems & Metadata

**BIAS & EXPLAINABILITY**

What is Bias: Definition, Types and Examples

Where it Occurs

How to Mitigate It

The Right to Explainability

**EVOLVING AI REGULATION**

Global

US

Oregon

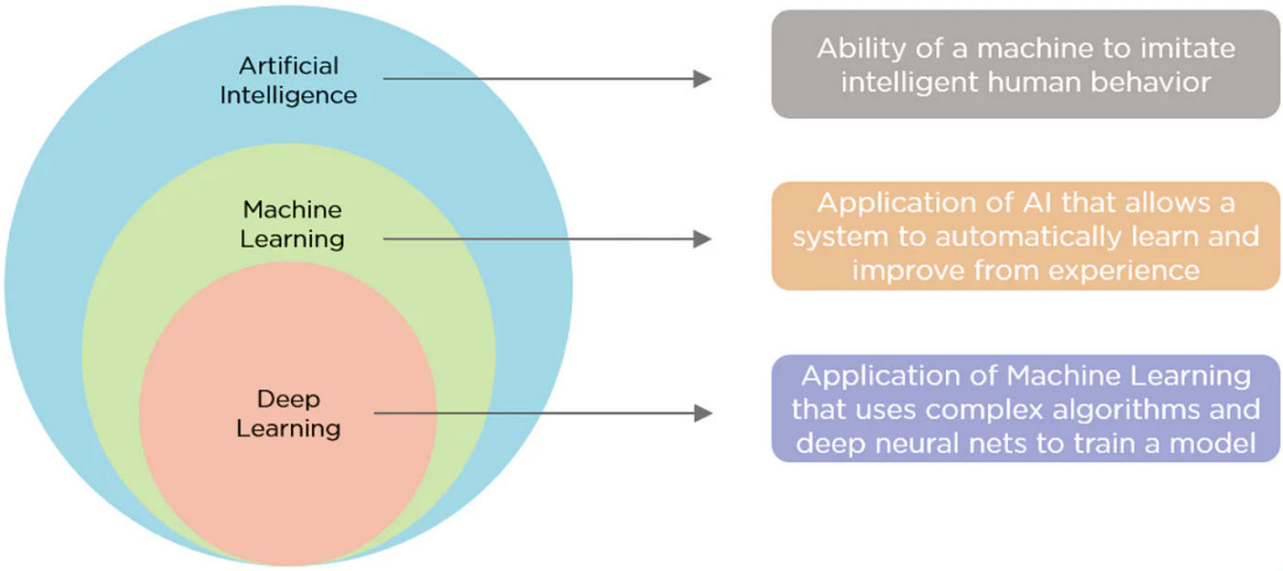
**ADDITIONAL RESOURCES**

**Q&A**

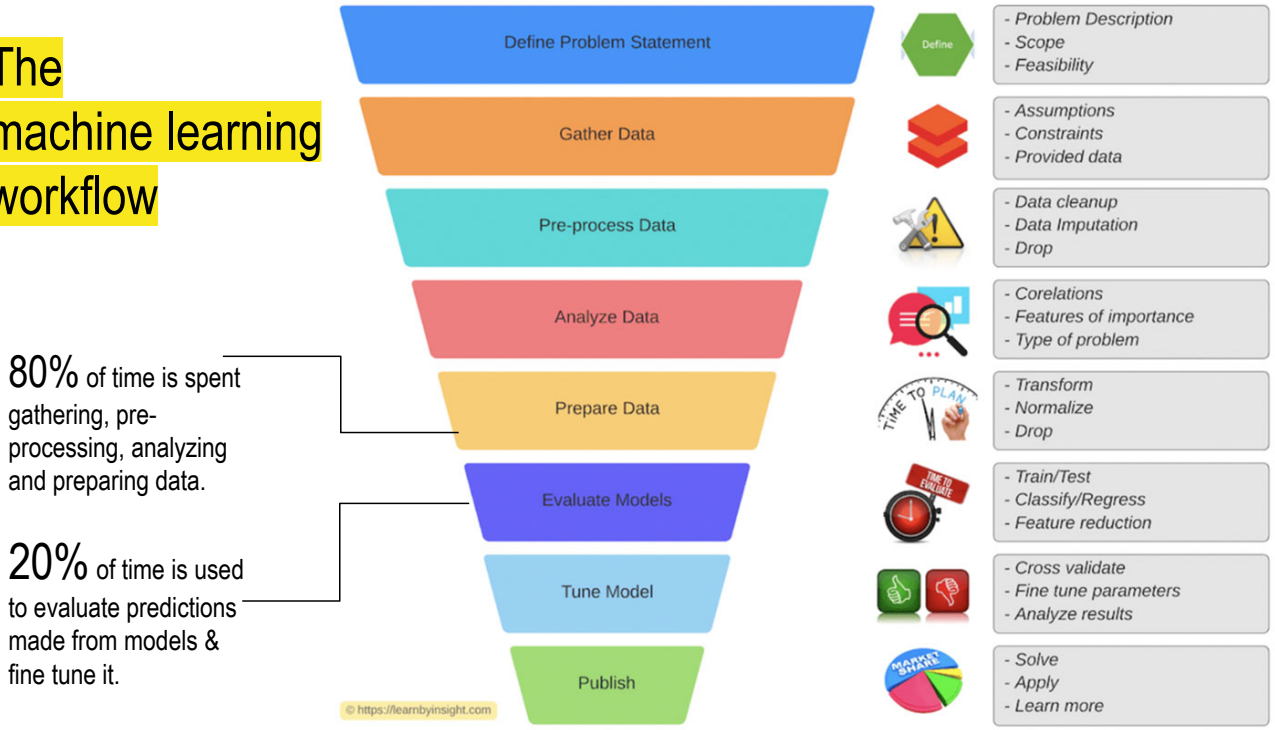
# Overview of AI

**Terms, Applications & Examples**

## Artificial intelligence vs. machine learning



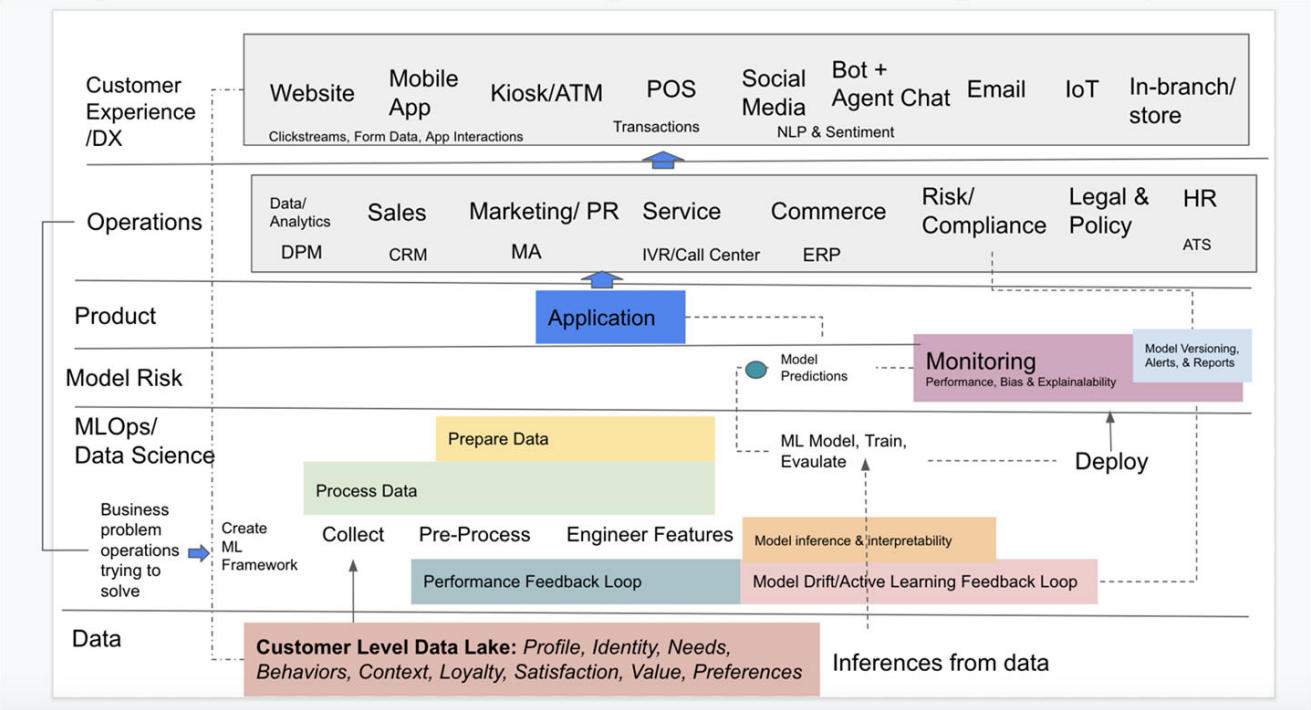

## The machine learning workflow




**80%** of time is spent gathering, pre-processing, analyzing and preparing data.

**20%** of time is used to evaluate predictions made from models & fine tune it.

## How personal data collected impacts end user experiences




## Real world applications of machine learning

well-known


(maybe) less well-known

## Deep Learning Examples:

**This Person Does Not Exist**
Use deep learning to present a random, computer generated photo of a fictional person.

**Tesla's Autonomous Driving Vehicles**
Use deep learning to recognize the space around a vehicle.

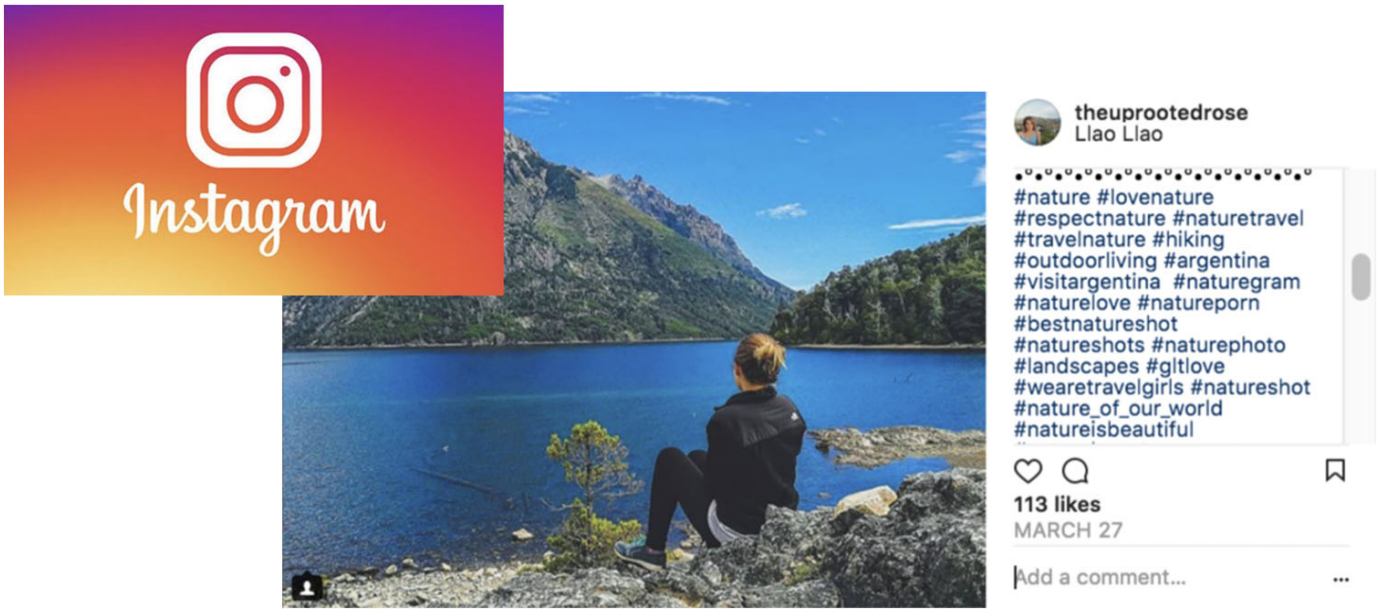

**Stable Diffusion Text to Image Generator**
Use deep learning for natural language processing (NLP) into visual art..

Prompt: kneeling cat knight, portrait, finely detailed armor, intricate design, silver, silk, cinematic lighting, 4k (Source)

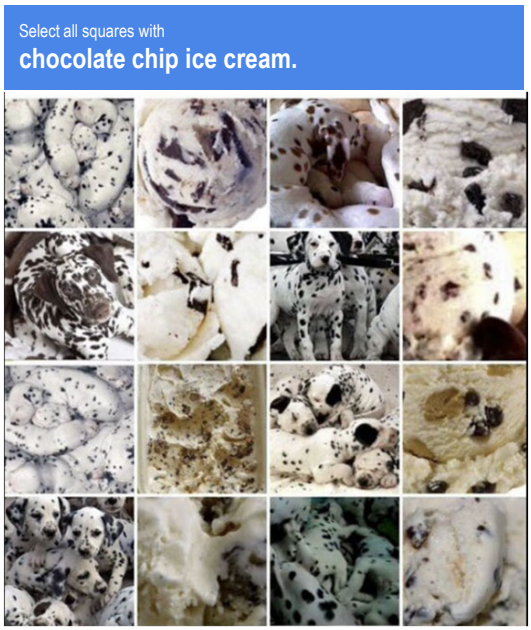
## Everyone trains machine learning systems daily.

**Hashtags, metadata, captcha**

## Metadata labeling




## Google CAPTCHA




## Metadata labeling for autonomous vehicles



# Bias

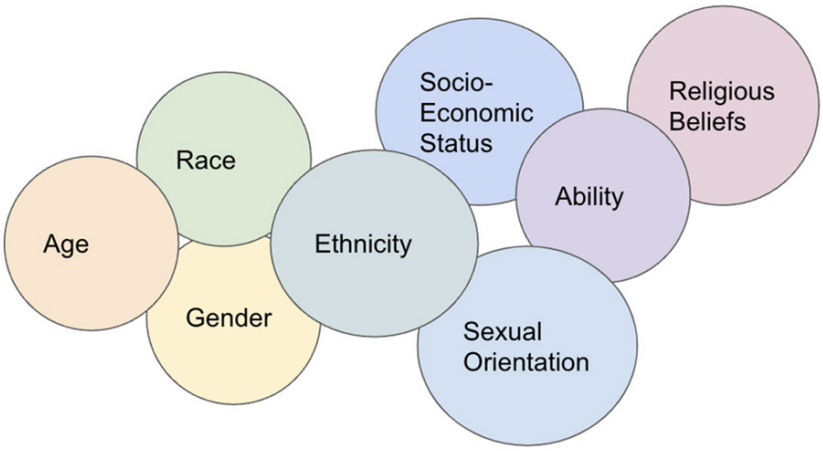
**What, Where, Why & How to Reduce It**

"The fear isn't that big data discriminates. We already know that it does. It's that you don't know if you've been discriminated against.
-Kate Crawford

What is AI Bias

The underlying **prejudice in data** that's **used to train machine learning algorithms**, which can ultimately **result in discrimination** and other social consequences.

## Protected Class Data

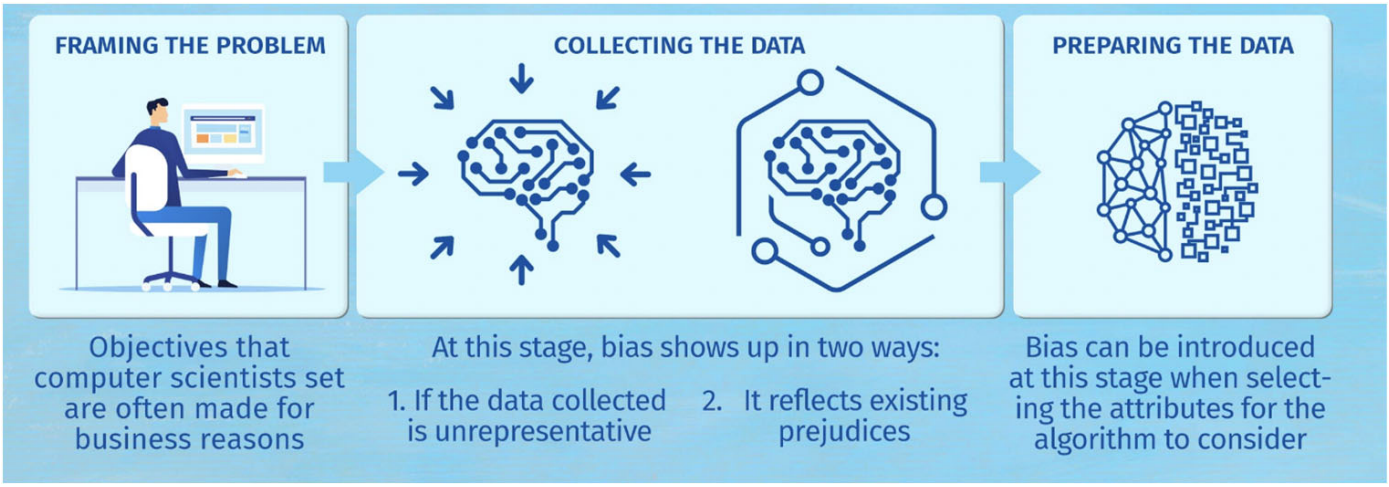



Protected classes of attributes should not be used in machine learning models but they are.

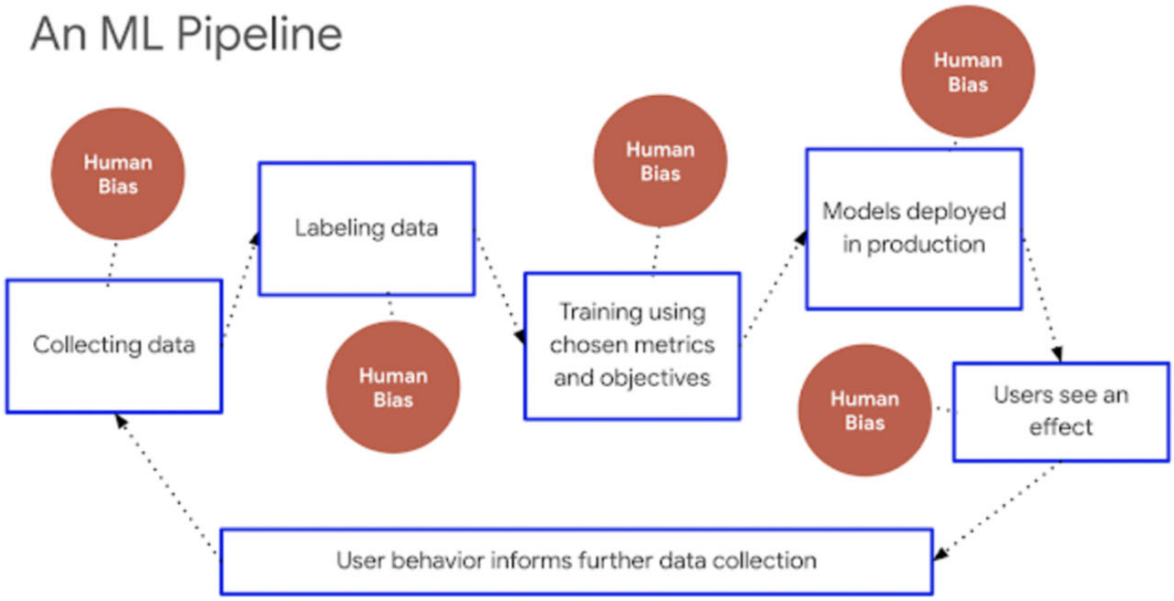
For example, **if age or race is used directly as a feature in an AI/ML model then the model is considered discriminatory** according to ECOA (Equal Credit Opportunity Act) as both age and race are protected attributes.

Even when these classes of attributes aren't being used in machine learning models, **discrimination may still exist through proxies.** Discrimination can be unintentional (disparate impact) or intentional (disparate treatment).

## Where does bias occur in machine learning worfklows?



## Humans are biased by nature and train machine learning models



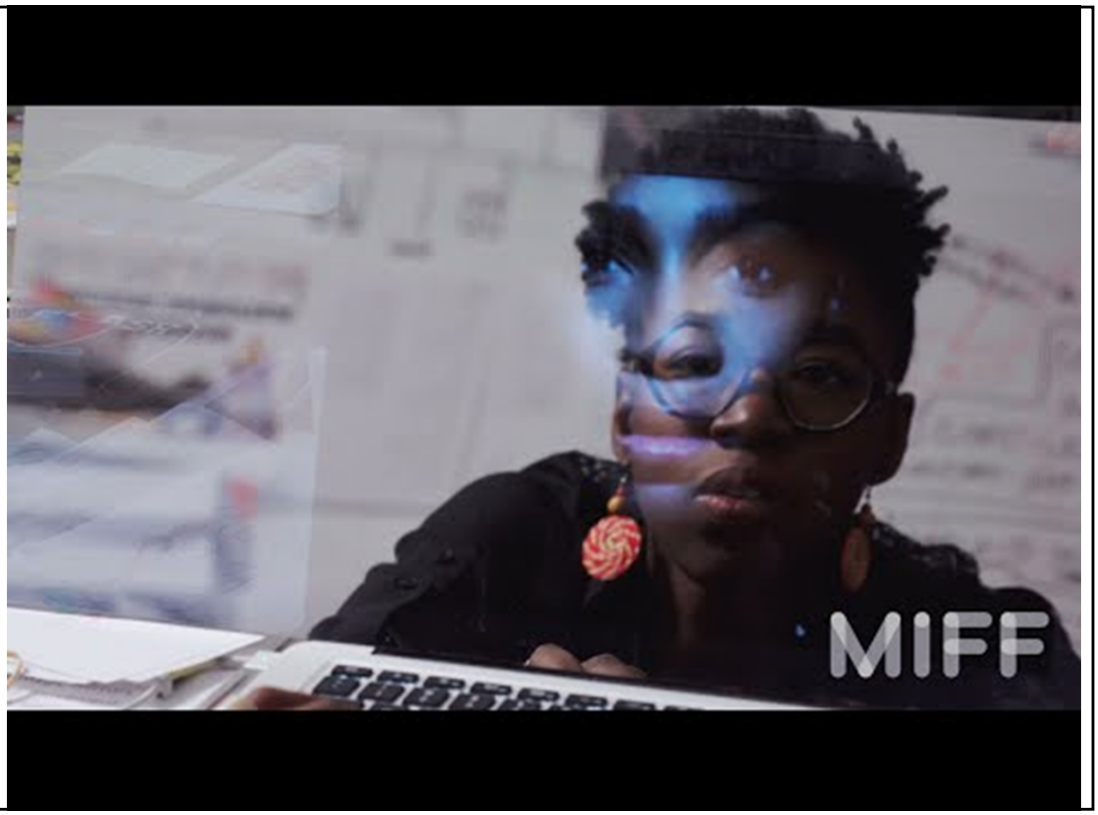

## Ways bias is amplified by AI

COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) is one of the most widely used algorithms in the U.S. criminal justice system and it has been applied or adapted by many states. It's algorithm is used in US court systems to predict the likelihood that a defendant would become a recidivist. Due to the data that was used, the model that was chosen, and the process of creating the algorithm overall, the model predicted twice as many false positives for recidivism for black offenders (45%) than white offenders (23%).

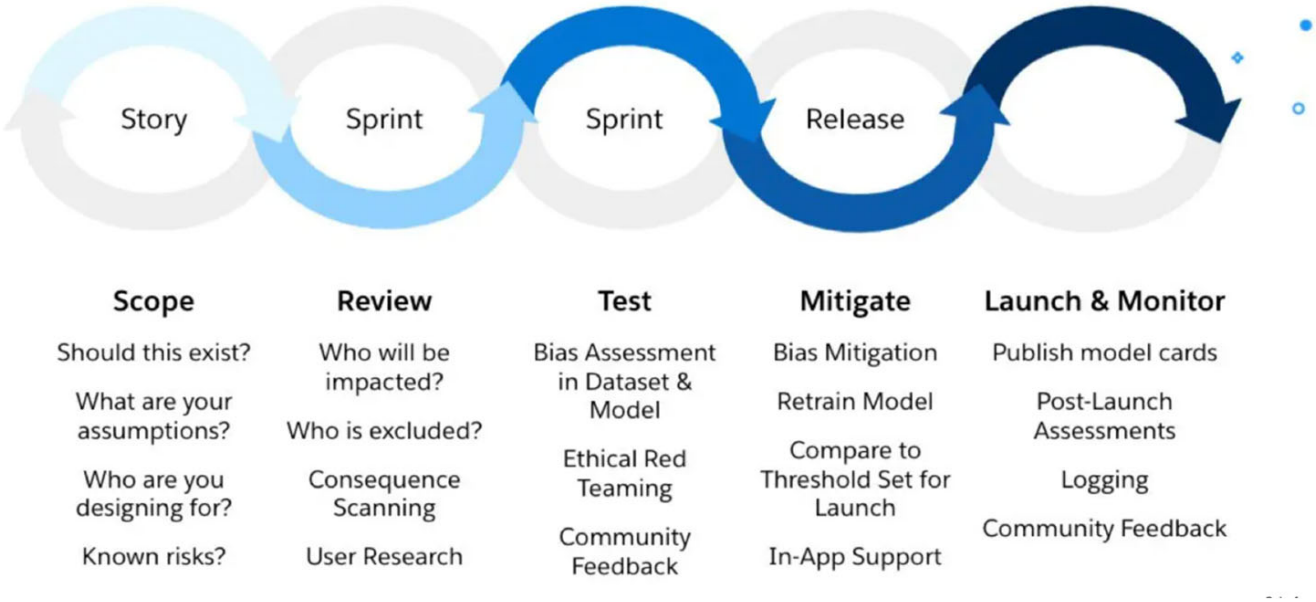
Amazon realized that their algorithm used for hiring employees was found to be biased against women. The reason for that was because the algorithm was based on the number of resumes submitted over the past ten years, and since most of the applicants were men, it was trained to favor men over women.

Older adults and their needs can become invisible to AI systems. In this way, AI systems reinforce inequality and magnify societal exclusion for sections of the population, creating a "digital underclass" primarily made up of older, poor, racialized and marginalized groups.

## Coded Bias: Netflix Documentary



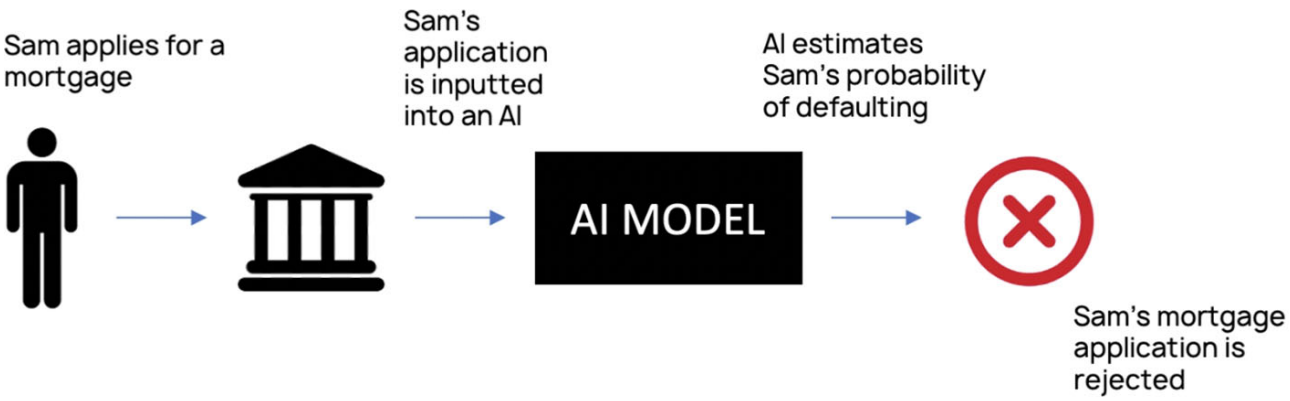

## Bias mitigation across the machine learning lifecycle



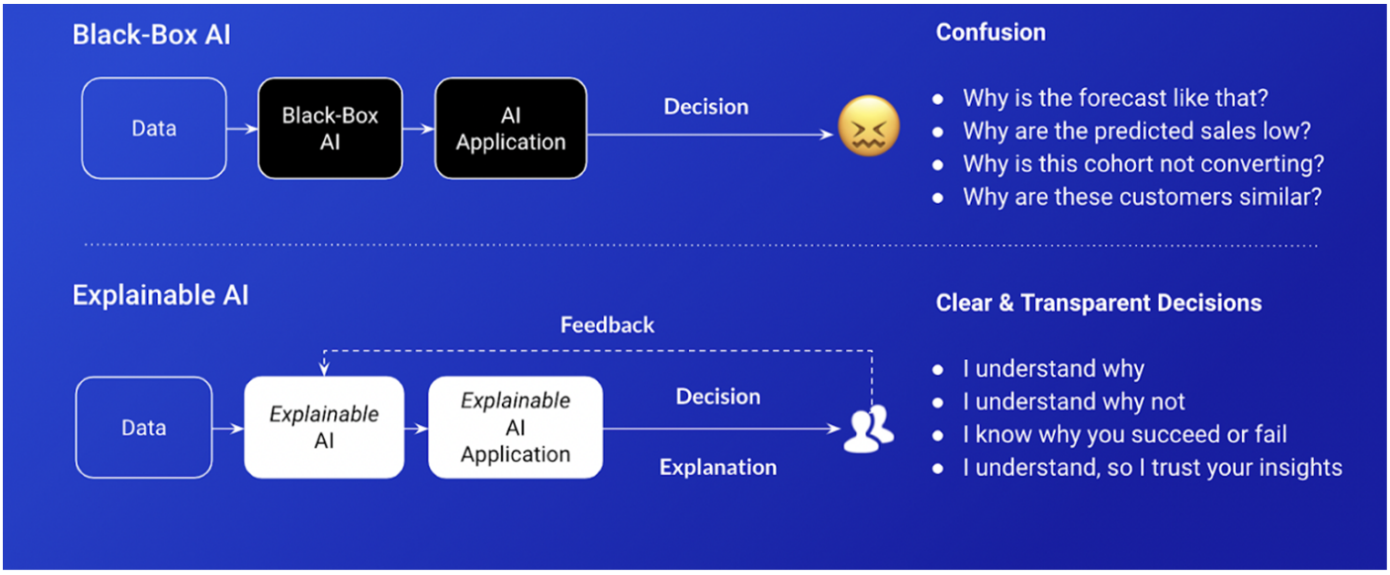
# Explainability (XAI)

**Understanding why AI made a decision**

## Why Explainability Matters



## Explanability answers why it happened, not how it happened




## Challenges with explainability

**150**

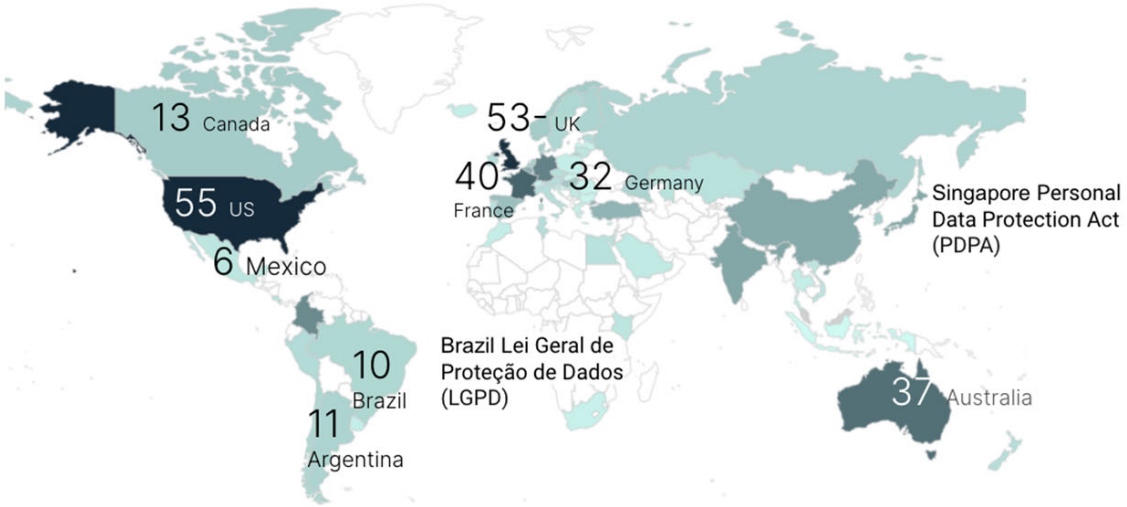
# Explainability Tools

**for implementing explainability algorithms**

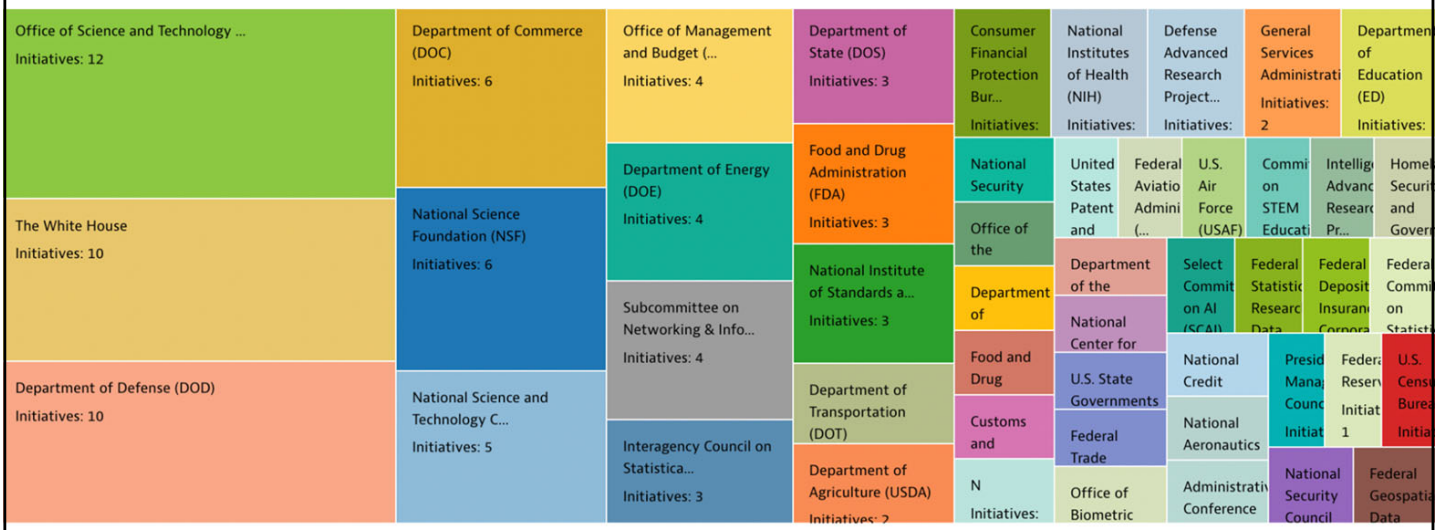
# Global & US AI Regulation

## How laws are evolving

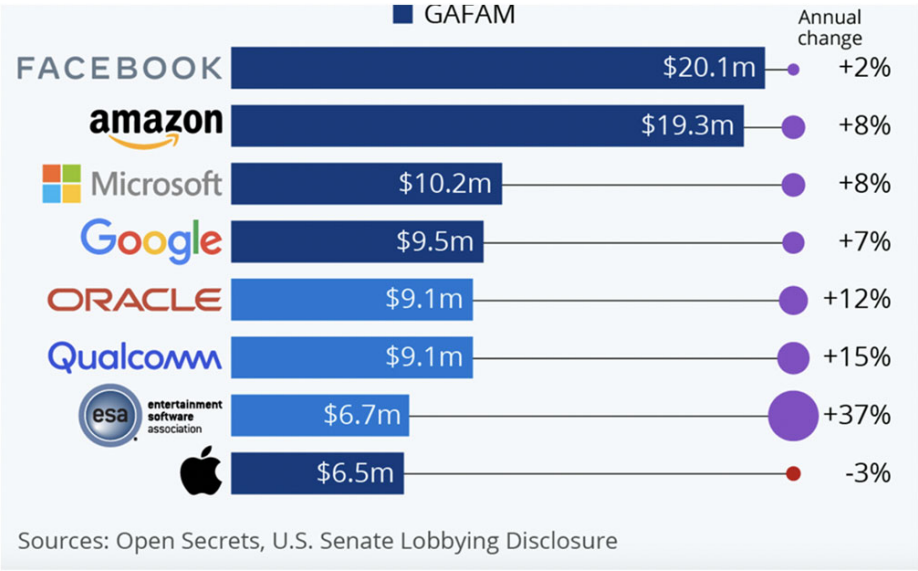
NO Universal standard for AI regulation worldwide.



## NO passed federal legislation in the US for AI regulation, currently.




## US Lobbying Against AI Regulation




**7 large tech companies** spent nearly **$70 million* lobbying the U.S. government in 2021.**

*Exceeds the **$65 million they spent in 2020**.

Heavy Influence across both parties and Congress to regulate the industry with weakened AI regulation.

# Oregon AI Regulation

**Facial recognition & autonomous vehicles**

## Facial Recognition

On January 1, 2021, Oregon became the first in the country to prohibit certain uses of facial recognition technologies by private entities in places of public accommodation.

Another ordinance banning the use and acquisition of face recognition technologies by all City of Portland bureaus and offices went into effect in September 2020.

Places or services offering to the public accommodations, advantages, facilities, or privileges," include:

- Hotels
- Restaurants
- Retail stores
- Recreation sites
- Public gathering locations

The definition is more sweeping than the 12 enumerated categories of public accommodations under Title III of the Americans with Disabilities Act.

## Example: Superior Court, State of New Jersey vs. Arteaga

**Case brief:**

*Armed robbery occurred on November 29, 2019.*

*Witnesses at the scene couldn't describe the robber.*

*New Jersey ran the video through their AI facial recognition system and got no match/results. Asked NYPD to run it through their AI facial recognition system and got a match using still images cropped from security cameras on the street.*

*It matched to Francisco Arteaga and he was arrested.*

*He claims he was never near the scene.*

**Electronic Privacy Information Center, the Electronic Frontier Foundation, and the National Association of Criminal Defense Lawyers submitted an amicus brief to the court to examine the AI, the potential for bias in those systems, and any human edits made as part of the legal discovery process.**

## Autonomous Vehicles (AV)

**Autonomous Vehicles have been involved in car crashes at 5x the rate of other cars.**

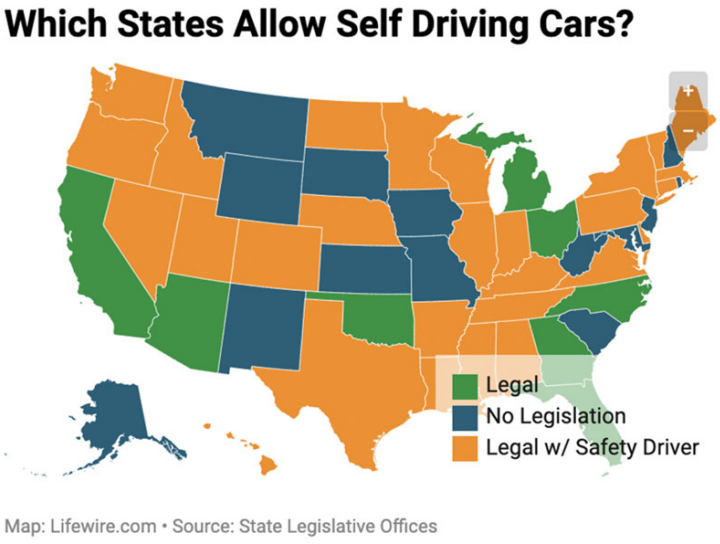
All these auto and ride sharing companies are testing AV within the state of Oregon.

Yet, Oregon lawmakers have not yet put laws in place requiring companies testing autonomous vehicles to report on planned tests in the state (notification is voluntary). While this might change in the future, currently Oregon residents are not warned when autonomous vehicles are being tested, whether on streets or highways.

## Self Driving Cars: Oregon vs. US

Oregon has legislation (HB 4063) that established an autonomous vehicle task force but it sunset-ed in January 2021.

This task force was responsible for developing recommendations for policies governing the use of self-driving cars in the state.




## Additional Resources

**Deepening your knowledge**

# AI Used in the Legal Profession

### JUDGE BOTS

Lex Machina

Using AI to **predicting legal outcomes.**

It allows an attorney to decide whether they should take a case on contingency, or how much to invest in experts, or whether to advise their clients to settle.

Use machine learning and predictive analytics to draw insights on individual judges and lawyers, as well as the legal case itself, to predict behaviors and outcomes.

### SUPER HUMAN LAWYERS

Lawgeex

Uses machine learning to **review contracts more quickly and consistently, spotting issues and errors** that may have been missed by human lawyers

CS Disco

Provide **AI-powered discovery services** to law firms across the US.

Quick Check

Uses AI to **analyze a draft argument to gain further insights or identify relevant authority** that may have been missed.

### AI-ENABLED SMART COURTS

China has been working to **build a 'smart court' system** since at least 2016 by incorporating Artificial Intelligence (AI) into its justice system.

The new system requires the **judges to consult AI on each case, and if they reject the AI's recommendation, they must provide a written explanation**.

AI had **cut a judge's average workload by over a third**, and saved Chinese citizens 1.7 billion working hours from 2019 to 2021.

# Deeper Dive

### WATCH

Coded Bias (Netflix)

The Great Hack (Netflix)

The Cleaners

Humans Need Not Apply

### READ

The Atlas of AI

The Alignment Problem

Weapons of Math Destruction

Algorithms of Oppression

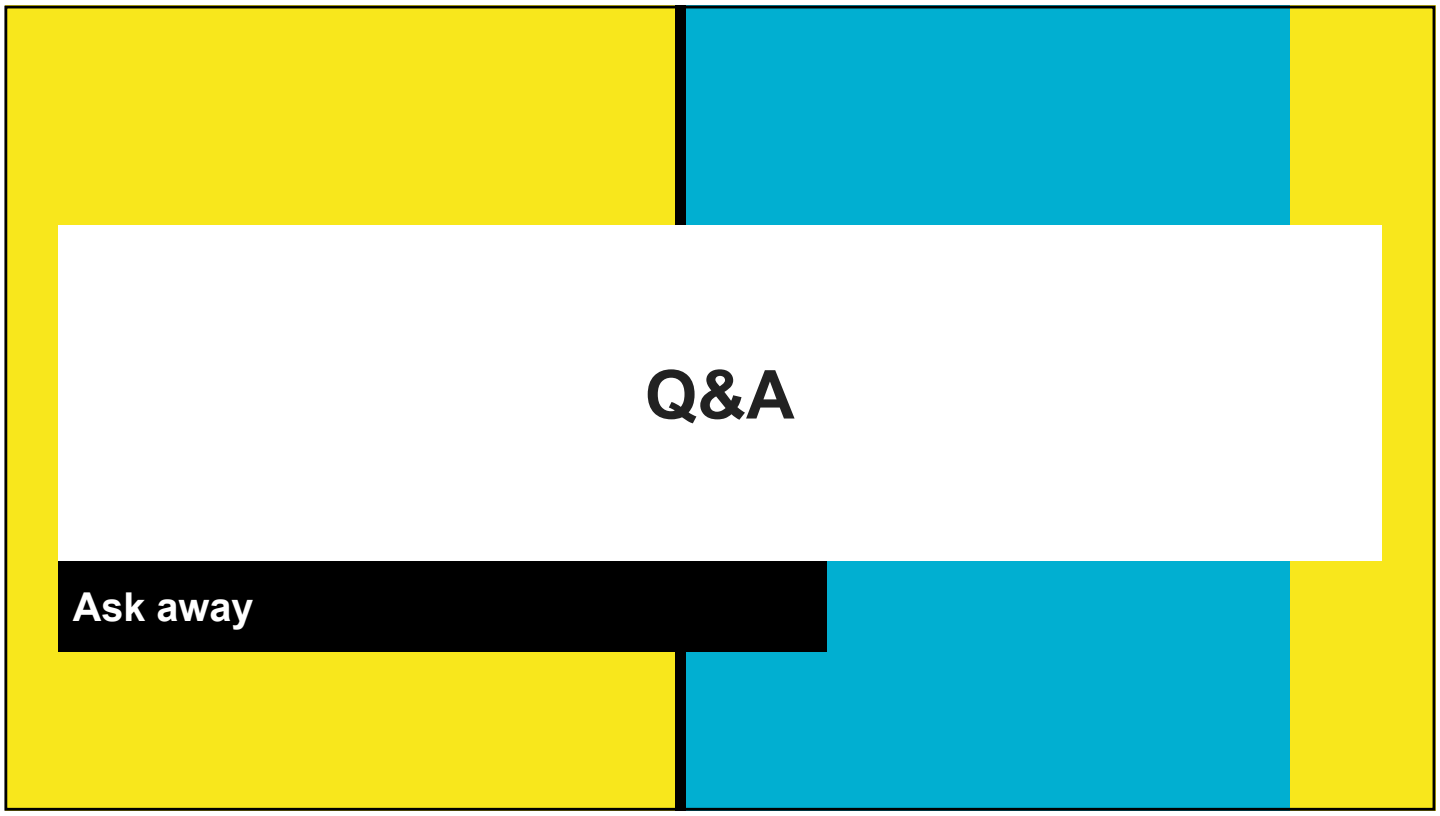
The Master Algorithm

### EXPLORE

Stable Diffusion Demo

Have I Been Trained?

How Normal am I?


Q&A
Ask away