AI, IoT, GPT, AND THE NEED FOR RESURGENT RIGHTS OF PRIVACY

Michael M. Losavio[*]

INTRODUCTION

Is it true that with modern technologies we have zero privacy and should "get over it?" Or does personal autonomy still hold sway? In 1999, the chief executive of a major computer vendor threw down the gauntlet, stating to workers and analysts that "you have zero

[*] Michael Martin Losavio teaches in the Department of Criminal Justice and the Department of Computer Science and Engineering at the University of Louisville, Louisville, Kentucky, U.S.A. on issues of law, society and information assurance in the computer engineering and justice administration disciplines.

privacy anyway" and should "get over it."[1] This led to denunciations by organizations ranging from the U.S. Federal Trade Commission to the Electronic Frontier Foundation.[2] But do we really have "zero privacy?" "Privacy" broadly covers external aspects of what control a person has over how they are viewed by others. An autonomous being may have rights as to her presentment to the world and the scope of that image of self. It is necessary, to some extent, to characterize and define what is meant by privacy.

"Privacy" has both internal and external components. The internal component relates to personal facts that a person may wish to and be entitled to keep from others.[3] The external component relates to aspects of a person's personality that they may have, to some extent, a right to control and validate.[4] This and other aspects of rights relating to privacy are seen in the discussion by the Office of the Australian Information Commissioner: "Privacy is a fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination. But it's hard to define. Different countries offer different views, as do individuals."[5]

Generally speaking, privacy includes the right to be free from (1) interference and intrusion, (2) to associate freely with whom you want, and (3) to control who can see or use information about you.[6] And there are different ways to look at privacy, such as: physical privacy (for instance, being frisked at airport security or giving a

[1] Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED MAG. (Jan. 26, 1999, 12:00 PM), https://www.wired.com/1999/01/sun-on-privacy-get-over-it [https://perma.cc/PU4E-YTV6] (reporting on comments of CEO Scott McNealy of Sun Microsystems at the launch ceremony for its new Jini technology).

[2] *Id*. Daniel Turner, "Evading the Google Eye " MIT TECHNOLOGY REVIEW, (Jan. 31, 2006), https://www.technologyreview.com/2006/01/31/229749/evading-the-google-eye-2/ [https://perma.cc/8KWV-YRP7]. Trivia, *Who was the Tech CEO that Back in 1999 Said, "You have Zero Privacy Anyway . . . ."*, TECHSPOT, https://www.techspot.com/trivia/127-who-tech-ceo-1999-you-have-zero-privacy/ [https://perma.cc/YC7N-5PCN] (last visited Mar. 25, 2025) (presenting Scott McNealy saying "You have zero privacy anyway. Get over it").

[3] Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 206 (1890).; Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 32 (1979).

[4] Brandeis & Warren, supra note 3.

[5] *What is Privacy?*, OFF. AUSTL. INFO. COMM'R, https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal information/what-is-privacy [https://perma.cc/3F6M-E8SC] (last visited May 13, 2024).

[6] *Id.*

bodily sample for medical reasons), surveillance (where your identity can't be proved or information isn't recorded), and information privacy (how your personal information is handled).[7]

This is an apt summary of the evolving topic of "privacy" in the world. Privacy can be considered a fundamental right relating to personal autonomy and respect. Privacy International describes it as:

> Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information. The rules that protect privacy give us the ability to assert our rights *in the face of significant power imbalances*.[8]

The birth and expansion of the Internet has a major impact on the power of information exchange and dissemination, creating its own opportunities for power imbalances. Its global connectivity and ease of information exchange given to the individual with access, currently estimated at 5.56 billion, expands the power of mass publicity to those individuals mediated only by their conscience.[9] Individuals may broadly disseminate information technology that is made easily accessible to all other individuals using the technology. That dissemination is largely unmediated by any regulatory body, vetting convention, or system of justice.[10] This has led to massive and global controversies regarding the obligations of those that may control such dissemination, to limit or bar the dissemination of injurious and false information.[11]

[7] *Id.*

[8] *Privacy*, PRIV. INT'L, https://privacyinternational.org/learn/privacy [https://perma.cc/6FT9-WL7F] (last visited Oct. 24, 2024) (emphasis added).

[9] *Number of Internet and Social Media Users Worldwide as of February 2025*, STATISTA, https://www.statista.com/statistics/617136/digital-population-worldwide/ [https://perma.cc/6MA3-5Z6B] (last visited Mar. 27, 2025).

[10] PRIV. INT'L, *supra* note 8; *see also* Anthony Varona, *Toward a Broadband Public Interest Standard*, 61 Admin. L. Rev., 1, 63, ,https://administrativelawreview.org/wp-content/uploads/sites/2/2014/04/Toward-a-Broadband-Public-Interest-Standard.pdf [https://perma.cc/ZT68-3JQB] (last visited Apr. 11, 2025).

[11] Jeffrey Howard, *The Ethics of Social Media: Why Content Moderation is a Moral Duty*, J. PRAC. ETHICS (2014), https://journals.publishing.umich.edu/jpe/news/153/ [https://perma.cc/26HZ-AJXK].

This egalitarian power for information dissemination is paralleled by the growth of sensing networks for data collection, cloud systems for preservation and storage of that data and artificial intelligence/machine learning systems for the rapid analysis of that data.[12] This vast number of devices generate data on the lives of others, increasing with each new system.[13] These range from cell phones, which nearly everyone possesses, to devices in the Internet of Things, which includes items ranging from toasters to automobiles.[14] Increasingly, every aspect of personal activity generates data that may be collected, stored in massive systems, and subject to increasingly sophisticated analyses.

Yet, in the past, the sheer volume of such information has tended to make its use difficult, often requiring a focused allocation of significant resources to delve through that data mass. Such an allocation itself limits analysis to special cases, such as persons of interest identified in criminal investigations.[15] This practical limitation has been overcome by applying machine learning and artificial intelligence systems to analyze large datasets, allowing for the identification of particular data on an individual and the generation of accurate inferences about those data subjects. The privacy given by the "practical obscurity" of massive data sets in hard-to-access forms can be undone by these systems.

This massive data collection and analytics erases boundaries that limit who has access to a person's information and removes controls a person may have over who may be allowed to access that information. It negates the ability to enforce rights against

[12] Dawn Kawamoto, *24 IoT Devices Connecting the World*, BUILTIN https://builtin.com/articles/iot-devices [https://perma.cc/RTA6-2ZJH] (last updated Aug. 13, 2024).

[13] *What is the Internet of Things?*, IBM.COM (May 12, 2023), https://www.ibm.com/think/topics/internet-of-things [https://perma.cc/KP4R-U78V].

[14] Scruthy, *18 Most Popular IoT Devices In 2025 (Only Noteworthy IoT Products)*, SOFTWARE TESTING HELP, https://www.softwaretestinghelp.com/iot-devices/ [https://perma.cc/UH36-TYL7] (last updated Mar. 18, 2025).

[15] *See, e.g.*, United States v. Jones, 565 U.S. 400, 403, 426 (2012) (Alito, J., concurring) (noting the potential impact of inexpensive mass tracking of individuals via computing technology).

imbalances in power between people and organizations as to support and protect personal autonomy.[16]

This intrusion has been massively expanded by the analytical capabilities of generative artificial intelligence to create false images and videos of anyone. Seeing may no longer be believing. I consider the interplay of law and technology and how it may guide a return to autonomy in the era of "Deep Fake" technology. We examine this in the context of "boundary condition" relating to the regulation of privacy in the United States.

I. THE LAWS OF THE UNITED STATES AS BOUNDARY CONDITIONS FOR TESTING

The people of the United States support a regime of greater information freedom than many other nations.[17] This freedom of information limits the ability to regulate conduct regarding information. This begins with the First Amendment to the founding document for the country, the Constitution of the United States, which prohibits the federal legislature from making any laws that abridge freedom of speech, the press, and the right of assembly.[18] The federal prohibition on infringement of the freedom of speech was extended to the individual states of the United States through the 14th Amendment to the Constitution.[19]

[16] Emily A. Vogels et al., *Power Dynamics Play a Key Role in Problems and Innovation*, *in* EXPERTS PREDICT MORE DIGITAL INNOVATION BY 2030 AIMED AT ENHANCING DEMOCRACY, PEW RES. CTR. (June 30, 2020), https://www.pewresearch.org/internet/2020/06/30/power-dynamics-play-a-key-role-in-problems-and-innovation/ [https://perma.cc/LX7R-N8V8].

[17] Richard Wike & Katie Simmons, *Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech: Americans Especially Likely to Embrace Individual Liberties*, PEW RES. CTR. (Nov. 18, 2015), https://www.pewresearch.org/global/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/ [https://perma.cc/Y7HB-2553].

[18] U.S. CONST. amend. I

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

[19] U.S. CONST. amend. XIV, § 1.

> All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State

For the United States, a concise description of privacy law is contained in the Second Restatement of Torts, which expertly summarizes four areas where privacy might be infringed to create liability. The four types of invasions are categorized as: (1) "unreasonable intrusion upon the seclusion of another;" (2) "appropriation of the other's name or likeness;" (3) "unreasonable publicity given to the other's private life;" and (4) "publicity that unreasonably places the other in a false light."[20]

The Restatement lays these out further:

> *Intrusion Upon Seclusion*: One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[21]
>
> *Appropriation of Name or Likeness*: One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.[22]
>
> *Publicity Given to Private Life*: One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[23]
>
> *False Light*: One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if the false light in which the other was placed would be highly offensive to a reasonable person, and the actor had knowledge of or acted in

shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

[20] RESTATEMENT (SECOND) OF TORTS §§ 652A-652I (AM. L. INST. 1977). The American Law Institute is drafting the Restatement (Third) of Torts on Privacy (US); *see also* Koeppel v. Speirs, 808 N.W.2d 177, 181 (Iowa 2011) (citing RESTATEMENT (SECOND) OF TORTS §§ 652A(2) (AM. L. INST. 1977)).

[21] RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

[22] *Id.* at § 652C.

[23] *Id.* at § 652D.

reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

The false representation must be "such a major misrepresentation of [the plaintiff's] character, history, activities or beliefs that serious offense may reasonably be expected to be taken by a reasonable man in his position . . . ."[24] Paralleling these invasions is the tort of outrageous conduct that causes severe emotional distress.[25]

The elements of that tortious misconduct are:

> (1) One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm. (2) Where such conduct is directed at a third person, the actor is subject to liability if he intentionally or recklessly causes severe emotional distress to (a) a member of such person's immediate family who is present at the time, whether or not such distress results in bodily harm, or (b) to any other person who is present at the time, if such distress results in bodily harm.[26]

Some states offer recovery for the negligent infliction of emotional distress via common law relief, subject to varying requirements of reasonable foreseeability, near-injury or actual physical injury. Section 282 of the Second Restatement of Torts, defines negligence as "conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm."[27] A framework of liability for the harms caused may now be built for the Internet, the Internet of Things, and AI.[28]

[24] *Id.* at § 652E, cmt. c.

[25] *Id.* at § 46.

[26] *Id.*

[27] Restatement (Second) of Torts § 282, (Am. L. Inst. 1977).

[28] Alberto Galasso & Hong Lou, *Risk Perception, Tort Liability, and Emerging Technologies*, BROOKINGS: RESEARCH, (Mar. 23, 2021), https://www.brookings.edu/articles/risk-perception-tort-liability-and-emerging-technologies/ [https://perma.cc/4NAU-SMDJ].

II. SO WHAT? HOW DOES AI, THE INTERNET, AND THIS NEW DATA LIFE CHANGE THINGS?

Human beings are creative at hurting others, and with each new technology, we try new ways to do so. The rise of the Internet, "Big Data," and Artificial Intelligence creates new ways to injure others. The malicious ecosystem made possible by these technologies is built on information, the transmission and collection of information, and its rapid analysis. The challenge, or question, is… to what end?

A. Publicity to Private Life and Publicity of False Light

Let us deconstruct the elements of privacy torts and how these technologies impact them. Publicity given to private life[29] and publicity as to cast someone in a "false light"[30] share two key elements: 1) publicity and 2) the information would be highly offensive to a reasonable person.[31] Publicity given to private life requires the additional element that the matter is not of legitimate concern to the public. However, false light requires a false portrayal of a person. Goldberg and Zipursky note the irony that while liability for *true* statements about private life may be actionable, liability for the *false* presentation of someone in a false light is controversial.[32] They suggest that, given the new technologies of the digital age, the tort of false light may be exactly the form of liability for injuries arising from these technologies.

Publicity given to private life requires: (1) publicity to; (2) a matter concerning the private life of another; (3) that would be highly offensive to a reasonable person, and; (4) is not of legitimate concern to the public.[33]

Similarly. false light elements require: (1) publicity; (2) to a matter concerning another; (3) that places the other before the public in a *false light* is subject to liability to the other for invasion

[29] RESTATEMENT (SECOND) OF TORTS § 652D, (AM. L. INST. 1977).

[30] *Id.* at § 652E.

[31] *Id.*

[32] John C. P. Goldberg & Benjamin C. Zipursky, *A Tort for the Digital Age: False Light Invasion of Privacy Reconsidered*, 73 DEPAUL L. REV. 461, 461-62 (2024).

[33] *Id.*

of his privacy, if; (4) the false light in which the other was placed would be highly offensive to a reasonable person.[34]

What may be deemed highly offensive may depend on the particular culture or society involved, so there may be variance between conduct in varied locations. Table 1 maps the elements of publicity in the first column and false light in the second column to particular Internet or computing technology involved in producing or transmitting information that effectuates violation of that particular element:

Table 1. Comparison of Technology's Contribution to Privacy Violations

Elements	**Tort of Publicity Given to Private Life**	**Tort of Publicity of False Light**	**Technology Contributing to Violation of Privacy**
1	publicity to	gives publicity	Internet & Social Media,
2	a matter concerning the private life of another	to a matter concerning another	OT, the Data, AI
3	that would be highly offensive to a reasonable person, and	that places the other before the public in a false light is	Artificial Intelligence
4	is not of legitimate concern to the public	the false light in which the other was placed would be highly offensive to a reasonable person	The Jury

[34] *Id.*

B. "Publicity" and the Technology at Issue

The element of "publicity" is more than the simple publication needed for a defamation action. Publicity requires broad dissemination of information at issue, but the technologies easily provide that capability. The global Internet and all of the information services built off of it create the foundation for easy publicity of any facts, including those that may be tortious. The only limitation may be that it must be a one-to-many dissemination rather than a single point-to-point e-mail or text message to a single person. And even such a single communication may still create liability since the technology can widely publicize this communication, spreading the damage done.

C. "Highly Offensive to a Reasonable Person" and the Technology at Issue

This element requires that the facts at issue are such that they would offend the sensibilities of a reasonable person, generally portraying the individual at issue in a very negative light. These elements differ since publicity given to private life relates to *true facts* of a private nature, the revelation of which is highly offensive to a reasonable person. False Light relates to facts that are *not true, are false,* and portray a person in a "false light," creating a false and untrue portrait that would be highly offensive to a reasonable person.[35]

For publicity given to private life by the technologies of the Internet of Things, data generation, the massive storage of so much of this information, and the analytical powers of artificial intelligence make the collection of facts in private life easy such that privacy-preserving technologies may become essential.[36] That

[35] *Id.*

[36] Kah Phooi Seng et al., *Artificial Intelligence Internet of Things: A New Paradigm of Distributed Sensor Networks*, INT'L J. 18 DISTRIBUTED SENSOR NETWORKS (2022), https://www.researchgate.net/publication/359198365_Artificial_intelligence_Internet_of_Things_A_new_paradigm_of_distributed_sensor_networks [https://perma.cc/9HLA-RDJS]; Lo'ai Tawalbeh et al., *IoT Privacy and Security: Challenges and Solutions*, 10 APPLIED SCIS. 4102 (2020), https://www.mdpi.com/2076-3417/10/12/4102 [https://perma.cc/AR2B-589B]; Franklin Oliveira et al., *Internet of Intelligent Things: A Convergence of Embedded Systems, Edge Computing and Machine Learning*, 26

power of surveillance, public and private, can feed facts into *analytical engines* that can produce information and inferences about information that, in the past, could not be easily accessed absent targeted surveillance.[37]

Further, the use of analytical systems such as GPT Artificial Intelligence can be tuned to precisely find or infer highly offensive facts to cause the most damage to the target of the revelations.[38] The systems can be further tuned to curate facts, whether private, true or false, for specific audiences that may be more sensitive to these matters, and thus, their revelation causes even greater harm to the subject of the information.[39]

D. "Matter Concerning Another" and the Technology at Issue

This refers to statements of fact that are identifiable and linked to a particular person other than the person generating and publicizing the information.[40] The difference made is that, arguably, a person can say as many bad or private things about themself to their heart's content, as long as it does not assert facts about another person.[41] Anything that attends to the human condition is collected from the myriad of devices and data collections on every aspect of the lives of others.

INTERNET OF THINGS (2024), https://www.sciencedirect.com/science/article/pii/S2542660524000945 [https://perma.cc/43CZ-R2BU].

[37] *See generally* Catarina Fontes, Ellen Hohma, Caitlin C. Corrigan, & Christoph Lütge, *AI-powered public surveillance systems: why we (might) need them and how we want them*, 71 TECH. IN SOC'Y, No. 71, November 2022, https://doi.org/10.1016/j.techsoc.2022.102137 [https://perma.cc/P72E-N6M3]

[38] *See, e.g.*, Assad Abbas, *Search Gets Smarter: How OpenAI's SearchGPT is Changing the Game*, UNITED.AI, (Sept. 11, 2024) https://www.unite.ai/search-gets-smarter-how-openais-searchgpt-is-changing-the-game/ [https://perma.cc/M9HV-HEU8].

[39] *Search GPT Prototype*, OPENAI, (July 15, 2024), https://openai.com/index/searchgpt-prototype.

[40] *Id.*

[41] *Id.*

For example, some of the most notorious examples of such privacy violations using these technologies come from the mouths of babies. Teenagers have been using the power of GPT AI systems for a variety of purposes. Some of the most malicious purposes relate to the ability of those systems to generate fake images, sometimes called "deepfakes." Such GPT programs include Midjourney,[42] Copilot Image Creator,[43] DaVinci AI,[44] DALL-E,[45] ChatGPT Image Generator[46] and a variety of similar programs. These all have the amazing power to create false but photorealistic images, sometimes using only text prompts to generate the images.

Some schools have faced great controversy because students created nude and pornographic images of another student that were publicized via Internet distribution or social media posting.[47] In one New Jersey high school, a firestorm erupted when sophomores generated false images of nude female students from their pictures found online through AI tools.[48] Those images were then shared through social media and other channels.[49] The humiliation and trauma those young women were subjected to was extensive.[50]

In this case, an immediate legal sanction may be possible via existing laws: punishment for the possession, manufacturing, and distribution of child pornography.[51] Although United States caselaw holds that virtual child pornography is not illegal (although it is in other countries), the use of real images of real children to create pornographic images is legal, even if they are content manipulations.[52] The children have become the subjects of child

[42] MIDJOURNEY, https://www.midjourney.com/home (last visited May 20, 2024).

[43] COPILOT, https://copilot.microsoft.com (last visited May 20, 2024).

[44] DAVINCI, https://davinci.ai (last visited May 20, 2024).

[45] DALL-E, https://openai.com/index/dall-e/ (last visited May 20, 2024).

[46] CHATGPT IMAGE GENERATOR, https://www.chatgptimagegenerator.org [https://perma.cc/EZ44-7S8F] (last visited May 20, 2024).

[47] *See, e.g.*, Julie Jargon, *Fake Nudes of Real Students Cause an Uproar at a New Jersey High School*, WALL ST. J. (Nov. 2, 2023, 7:00 AM), https://www.wsj.com/tech/fake-nudes-of-real-students-cause-an-uproar-at-a-new-jersey-high-school-df10f1bb [https://perma.cc/N8YC-ULQZ] (describing incident involving students' use of artificial intelligence to generate fake nude photos of classmates that circulated in their school).

[48] *Id.*

[49] *Id.*

[50] *Id*

[51] 18 U.S.C. § 2251; *see also* 18 U.S.C. § 2252.

[52] *See generally* Ashcroft v. Free Speech Coal., 535 U.S. 234 (2002).

sexual abuse material via these technologies and victims of emotional abuse caused by such images and their distribution.[53]

Civil liability for such actions is found in the privacy torts discussed herein. In particular, the tort of False Light is applicable here. The creation and distribution of images showing female students in pornographic images place those female students in a false light as to their conduct and morals. Depiction of such images of young female students and their distribution, particularly as these are without permission, is highly offensive to a reasonable person. To a reasonable parent, such conduct might lead that parent to pursue retribution against the creator and distributor of the materials humiliating their child.

Such abuse can expand further into image manipulation involving adults. Again, the False Light tort may be a key civil remedy, perhaps accompanied by defamation. There are differences of opinion as to whether these could be applied to such image abuse as to sexual matters, but a foundation of liability can be built.

False Light requires publicity via distribution, but the tort of intentional or negligent infliction of emotional distress may be used to address efforts where publicity cannot be shown. This may be appropriate when the motive for the image generation is for malicious purposes other than torment to establish attempts at extortion.

III. DEEPFAKES OF CRIMINAL CONDUCT

The injuries from deepfake images extend well beyond humiliation and public disdain. The laws relating to evidence in criminal cases show the risks at issue. For example, where an image is connected as coming from a person, it may be a powerful admission of liability. However, the corroboration rule is a rule of reliability that avoids errors in convictions based upon untrue statements, and it promotes sound law enforcement by requiring police investigations to extend their efforts beyond the words of the accused.[54] This ensures that an appropriate investigation is done

[53] *Child Sexual Abuse Material Created by Generative AI and Similar Online Tools is Illegal*, FED. BUREAU INVESTIGATION (Mar. 29, 2024), https://www.ic3.gov/PSA/2024/PSA240329 [https://perma.cc/MRY2-PQYS].

[54] *See* Wong Sun v. United States, 371 U.S. 471, 489 (1963); *see also* Smith v. United States, 348 U.S. 147 (1954).

prior to prosecution.[55] The government may corroborate by substantial evidence apart from the defendant's admissions.[56] "An out-of-court admission is adequately corroborated if the corroborating evidence 'supports the essential facts admitted sufficiently to justify a jury inference of their truth.'"[57]

In *Opper v. United States*, the Supreme Court considered extra-judicial statements made by an accused that were "admissions of essential facts or elements of the crime" and concluded that they were "of the same character as confessions and that corroboration should be required."[58] The quanta of corroboration was set out therein:

> [W]e think . . . that the corroborative evidence need not be sufficient, independent of the statements, to establish the corpus delicti. It is necessary, therefore, to require the Government to introduce substantial independent evidence which would tend to establish the trustworthiness of the statement. Thus, the independent evidence serves a dual function. It tends to make the admission reliable, thus corroborating it while also establishing independently the other necessary elements of the offense. It is sufficient if the corroboration supports the essential facts admitted sufficiently to justify a jury inference of their truth. Those facts plus the other evidence besides the admission must, of course, be sufficient to find guilt beyond a reasonable doubt.[59]

[55] *Smith*, 348 U.S. at 152.

[56] *Id.* at 157.

[57] United States v. Pennell, 737 F.2d 521, 527 (6th Cir. 1984) (quoting Opper v. United States, 348 U.S. 84, 92-93 (1954)).

[58] *Opper*, 348 U.S. at 90.

[59] *Id.* at 93 (citation omitted); *see also Smith,* 348 U.S. at 155 ("An admission which assumes this importance in the presentation of the prosecution's case should not go uncorroborated, and this is true whether we consider the statement an admission of one of the formal 'elements' of the crime or of a fact subsidiary to the proof of these 'elements.'")

Based on these cases, there is some protection where a deep fake is considered a statement from the party featured. But if it is considered third-party evidence of misconduct, what then protects against deep fake abuse? Issues of deep fake impersonation have been raised in courts. Child pornography criminal statutes have been challenged due to issues of deep fake generation.[60] In *U.S. v. Tatum*, the question of liability arose precisely because of the use of deep fake generators:

> The Defendant agreed to speak with the FBI agents in the parking lot. During this conversation the Defendant allegedly admitted that: (1) he and Kimberly shared the MacBook laptop; (2) he would obtain images of teen girls from a website called "teen gallery" and input the image in a "deep fake" website, which would make the girl in the image appear nude; (3) it was possible that a reasonable person might think the girls were under the age of 18; (4) he masturbated to a "deep fake" nude photograph of an ex-girlfriend (who was a minor at the time of the photograph); and (5) he saved these images to zip drives or thumb drives.[61]

Despite the defendant's arguments, he was convicted and sentenced to forty years imprisonment.[62] Another challenge to criminal liability in this age of manipulation, *Newell v. Barr*, was dismissed.[63] The plaintiff there argued that:

[60] Newell v. Barr, No. CV 19-06893-CJC(AGRx), 2021 U.S. Dist. LEXIS 112237, at *1 (C.D. Cal. June 15, 2021).

[61] United States v. Tatum, No. 3:22-CR-00157-KDB-DCK, 2023 U.S. Dist. LEXIS 75482, at *3-4 (W.D.N.C. May 1, 2023).

[62] *Id.*

[63] *Newell*, 2021 U.S. Dist. LEXIS 112237, at *3.

> [M]y complaint seeks only one thing: an affirmation of the constitutional principles articulated in *Ashcroft v. Free Speech Coalition* for the *deep fake* era, which the Government violates daily with certain ongoing child pornography prosecutions. To do so, my complaint relies on other, prior case law that must be applied to the new—and constitutionally significant—development of deep fakes.[64]

Though dismissed, this action demonstrates the growing intrusion of deep fake possibilities into the way some view the reality of the world.

IV. FURTHER ISSUES

The power of AI to analyze massive databases of information on people extends to the inferences those systems may make. AI is a huge probability engine that looks at data and patterns that appear within the corpus of data it digests and then makes inferences from that pre-existing information. The use of this power of AI may invoke both issues relating to the publicity of private facts and the publicity of false facts to depict someone in a false light. In one instance, a law professor was "accused" by a GPT AI of sexual misconduct, an accusation that was completely false but responded to the AI system's mandate to provide an answer.[65] Publication of this may be actionable defamation with no excuse that "the machine made me do it!"[66]

[64] *Id.* (emphasis in original).

[65] Pranshu Verma & Will Oremus, *ChatGPT Invented a Sexual Harassment Scandal and Named a Real Law Prof as the Accused*, WASH. POST, (Apr. 5, 2023, 2:07 PM), https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/ [https://perma.cc/5V4P-LGPZ].

[66] Joel Simon, *Can AI be Sued for Defamation?*" COLUM. JOURNALISM REV. (Mar. 18, 2024), https://www.cjr.org/analysis/ai-sued-suit-defamation-libel-chatgpt-google-volokh.php [https://perma.cc/5VX2-SBP9].

A. Appropriation of Name or Likeness

Lurking at the fringes of liability is the notion that the appropriation of a person's name or likeness is actionable: one who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.[67] This suggests the possibility of tort liability in the way that GPT AI systems are trained.[68] The algorithmic engine analyzes huge amounts of data to look at probability distributions and patterns from which it can then extrapolate an appropriate production, whether it be words, images or video.[69] There has been considerable controversy over possible copyright violations in using this data to train the system. AI manufacturers contend training their systems is fair use of the data as there is no impact on the commercial value of such data; as a "fair use," there is no copyright violation by their training of their systems.[70] Beyond this, however, is that the AI systems do not yet seem to have appropriate discrimination as to their output.[71] The most notorious examples of this are what have been called "AI Hallucinations," where, in order to meet the system's mandate to produce something, it outputs completely spurious information.[72] This might include claiming a particular person as an author or using the image of someone in the computed output of the system.

[67] RESTATEMENT (SECOND) OF TORTS § 652C (AM. L. INST. 1977).

[68] Andrew Myers, *Reexamining "Fair Use" in the Age of AI*, STAN. UNIV. HUMAN-CENTERED A.I. (June 5, 2023) https://hai.stanford.edu/news/reexamining-fair-use-age-ai [https://perma.cc/BGN5-9NZ7] ("Generative AI claims to produce new language and images, but when those ideas are based on copyrighted material, who gets the credit?").

[69] *Id.*

[70] Roomy Khan, *AI Training Data Dilemma: Legal Experts Argue for 'Fair Use'*, FORBES: MONEY (Oct. 4, 2024, 12:24 PM), https://www.forbes.com/sites/roomykhan/2024/10/04/ai-training-data-dilemma-legal-experts-argue-for-fair-use/ [https://perma.cc/M7HX-FKTF].

[71] *When AI Gets It Wrong: Addressing AI Hallucinations and Bias*, MIT SLOAN TEACHING & LEARNING TECHS., https://mitsloanedtech.mit.edu/ai/basics/addressing-ai-hallucinations-and-bias [https://perma.cc/K32Z-272H]. (last visited Nov. 3, 2024) (discussing inherent challenges in AI Design where " [t]he technology behind generative AI tools isn't designed to differentiate between what's true and what's not true.")

[72] *Id.*

A notable example regarding practice of law involved lawyers who submitted a GPT-generated legal brief to a court of law.[73] Some of the cases cited by the GPT system simply did not exist, although they appeared legitimate and cited particular judges as the authors of those nonexistent opinions. In addition to financial penalties, the lawyers were directed to write letters of apology to the named judges noted in the opinions explaining what they had done.[74]

Another potential source of liability from the power of the systems may lie in the tort of the intrusion upon the seclusion of a person.[75] The Restatement (Second) defined this as follows: "One who intentionally intrudes, physically or *otherwise*, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[76]

This creates liability for someone who intentionally intrudes into the private affairs of another where such an intrusion is highly offensive to a reasonable person.[77] While this tort is founded on physical intrusion, it covers intrusions that are "physical or *otherwise*."[78] This reflects an attention to modern technologies that can invade the solitude or seclusion of someone without a physical trespass.

Such attention to modern technologies was evidenced in an instance where it was found to be an unlawful invasion of privacy in violation of the Fourth Amendment to use an infrared imaging device to look into the activities of a person's home.[79] This was further seen in finding that a Fourth Amendment violation

[73] Debra Cassens Weiss, *Judge Finds Out Why Brief Cited Nonexistent Cases—ChatGPT Did Research*, ABA J.: A.I. & ROBOTICS, (May 30, 2023, 12:30 PM) https://www.abajournal.com/news/article/judge-finds-out-why-brief-cited-nonexistent-cases-chatgpt-did-the-research [https://perma.cc/H58G-75XD].

[74] Jon Brodkin, *Lawyers Have Real Bad Day in Court After Citing Fake Cases Made Up by ChatGPT*, ARS TECHNICA, (June 23, 2024, 12:32 PM) https://arstechnica.com/tech-policy/2023/06/lawyers-have-real-bad-day-in-court-after-citing-fake-cases-made-up-by-chatgpt/#gsc.tab=0 [https://perma.cc/L75C-8MYK]; Benjamin Weiser, *ChatGPT Lawyers Are Ordered to Consider Seeking Forgiveness*, NEW YORK TIMES (June 22, 2023) https://www.nytimes.com/2023/06/22/nyregion/lawyers-chatgpt-schwartz-loduca.html [https://perma.cc/U9A6-AAM5].

[75] *What is Privacy?*, OFF. AUSTL. INFO. COMM'R, *supra* note 5.

[76] RESTATEMENT (SECOND) OF TORTS § 652BC (AM. L. INST. 1977) (emphasis added).

[77] *Id.*

[78] *Id.*

[79] Kyllo v. United States, 533 U.S. 27, 27 (2001).

occurred when law enforcement accessed databases to create a locational profile of an individual from cell phone information and cell site historical information without a warrant from a court.[80]

The use of the inferential power of AI creates a host of questions regarding a variety of issues and its ability to reveal a person's private affairs or concerns solitude or seclusion. Concern about this particular invasion of privacy is heightened when viewed through the lens of the Fourth Amendment to the United States Constitution. The Fourth Amendment is meant to control actions by state officers by requiring probable cause that a crime has occurred or that evidence crime will be found in relation to a particular person or that person's home, office or other place.

The issues relating to this inferential power are the same as those in *Carpenter v. United States.*[81] *Carpenter* set aside a long-standing principle that an individual does not have information about him or her that is maintained by third-party. The United States Supreme Court set aside that long-standing exception through an extensive analysis of how modern data technologies, the sensing device presented by a cell phone, and ease of analytics could reveal any facts of private life, such as where one goes or with whom one associates.

The challenge of authenticating image and video sources will grow as more and more of these artifacts are used to hurt others. A clear standard and process of authentication, beginning with judicial process, is needed.

CONCLUSION

Law is applied to the facts to achieve a resolution of some dispute, particularly where someone is injured. The new facts of AI, GPT and IOT are still subject to the law, especially where someone is injured. Careful analysis of these new facts of these new technologies will aid in the application of legal principles, from civil liability to criminal sanctions.

The impacts of these new technologies, dealing with information and its analysis, must be examined in light of the law of privacy. This is especially important for the torts of False Light,

[80] Carpenter v. United States, 585 U.S. 296, 296-97 (2018).

[81] *Id.*

revelation of Private Facts not of concern to the public, technical intrusion upon the seclusion of an individual, and misappropriating the identity of someone. These are all detailed in the Restatement of Torts (Second), now under review and revision for a new restatement. The importance of this examination is further seen in the torts of negligent and intentional infliction of emotional distress and defamation where these technologies are used to hurt others.

Legislative efforts are underway to provide new statutory protections for privacy from these outrageous offenses perpetrated on people. This legislation must be judged against the protections of the United States Constitution and the Bill of Rights. The interests this new legislation seeks to protect may be of such compelling interest to a fair and just society that it passes constitutional muster. Our challenge is designing such protective regulation without limiting the great benefits these new information technologies offer.