THESE ARE NOT THE DROIDS YOU ARE LOOKING FOR: THE URGENT NEED FOR STATE REGULATION OF ARTIFICIALLY INTELLIGENT SEX ROBOTS

Dan Lev[*]

Abstract

The advancement of technology makes the creation of Artificially Intelligent sex robots (Sexbots) an inevitability within the foreseeable future. Sexbots present a unique challenge to legal structures because they will implicate laws governing third-party data sharing, biometric information, freedom of expression, sex toy regulation, and artificial intelligence (AI). After examining state laws governing AI and data privacy, it is clear neither Illinois law nor federal law is prepared to effectively govern the issues of the present, let alone the future. This Note argues Illinois should adopt wider-encompassing data privacy laws, draft stronger consumer protection laws modeled after other states, and establish an AI framework that provides oversight to how AI algorithms are drafted and executed. This Note explores the multitude of legal doctrines Sexbots may implicate and examines state, federal, and international laws governing data privacy and AI.

TABLE OF CONTENTS

* J.D. Candidate, University of Illinois College of Law, 2023; B.A., Oberlin College, 2017. This Note would not be possible without the incredible people in my life. To my parents, for always encouraging me to be myself. To the Champaign Yacht Authority, for making law school tolerable. Lastly, to Jubes, for hooking it up fatty style.

I. INTRODUCTION

Imagine this: robots infused with artificial intelligence (AI) capable of having sexual intercourse with humans. Believe it or not, these robots are already here.[1]

Humans have come a long way from sculpting phalluses out of siltstone twenty-eight thousand years ago.[2] Now, sex toys are designed by medical professionals, sexual educators, and design specialists,[3] and the global sex toy market is currently valued at approximately thirty-seven billion dollars.[4] The introduction of AI sex robots (Sexbots) represents the next frontier in the sexual

1. *See* Lizzie Crocker, *What Sex Robot Should You Order*, DAILY BEAST (Aug. 19, 2017, 12:01AM), https://www.thedailybeast.com/what-sex-robot-should-you-order [perma.cc/2TCZ-7V2D] (describing how robots with artificial intelligence capacities for sexual intercourse are currently on the market).

2. Jonathan Amos, *Ancient Phallus Unearthed in Cave*, BBC NEWS (July 25, 2005, 12:04 PM), http://news.bbc.co.uk/2/hi/science/nature/4713323.stm [perma.cc/ZB88-ZEZA] ("The 20cm-long, 3cm-wide stone object, which is dated to be about 28,000 years old, was buried in the famous Hohle Fels Cave near Ulm in the Swabian Jura. The prehistoric 'tool' was reassembled from 14 fragments of siltstone.").

3. Jaina Grey & Louryn Strampe, *The Best Sex Toys for Every Body*, WIRED (Sept. 18, 2022, 9:00 AM), https://www.wired.com/gallery/best-sex-toys-and-tech [perma.cc/S4KA-RYKT] ("Today's toys are designed by sex educators, medical professionals, and some of the world's greatest sexperts.").

4. *Size of the Sex Toy Market Worldwide from 2016 to 2030*, STATISTA (July 2, 2022), https://www.statista.com/statistics/587109/size-of-the-global-sex-toy-market [perma.cc/FT8P-MCLN] (providing statistical information on the market size of the worldwide sex toy market).

device evolution; and it presents technical, ethical, and regulatory issues for the industry, its clients, and society.

Currently, AI Sexbots are able to draw from an array of preprogramed responses to fit a handful of general archetypes.[5] While this is more technologically sophisticated than a non-sentient inflatable latex doll, it is likely closer to the doll than it is to Hollywood interpretations of futuristic robot sex machines.[6] But what happens when Sexbot technology inevitably advances? Instead of a low sophistication robot being able to respond in dozens of preprogrammed ways from a few archetypes, how will society adapt to the equivalent of Apple's Siri[7] or Amazon's Alexa[8] occupying the body of host from HBO's Westworld?[9]

The relationship between humans and robots is already showing signs of emotional growth. As early as 2007, it was noted that people were able to form emotional bonds with their vacuum cleaners.[10] Current forecasts suggest that people would be open to human-robot intimacy.[11] In an international survey conducted in March 2017, seven percent of women and eleven percent of men said they would be open to dating a robot.[12] Additionally, over a quarter of millennials polled said humans will eventually form deep friendships and emotional relationships with machines.[13]

While it is true that technology has always advanced and humans have always adapted to these developments, AI is different. The wheel or the printing press certainly serve as examples of technology that changed human productivity, economics, and society, but at their core they did not change human nature.[14] In a study from Yale, human participants played a game

5. John Danaher, *Should We Be Thinking About Robot Sex? in* ROBOT SEX: SOCIAL AND ETHICAL IMPLICATIONS 1, 6–8 (John Danaher & Neal McArthur eds., 2017).

6. HER (Annapurna Pictures 2013); BLADE RUNNER 2049 (Columbia Pictures et al. 2017); TRON: LEGACY (Walt Disney Pictures & Sean Bailey Productions 2010).

7. *Siri*, APPLE, https://www.apple.com/siri [perma.cc/UCV9-DNRR] (last visited Oct. 5, 2022).

8. *What is Alexa?*, AMAZON, https://developer.amazon.com/en-US/alexa [perma.cc/X2CK-QJL6] (last visited Oct. 5, 2022).

9. *Westworld: The Maze* (HBO television broadcast Oct. 2, 2016).

10. Ja-Young Sung et al., *"My Roomba Is Rambo": Intimate Home Appliances*, 2007 UBIQUITOUS COMPUTING 145, 147 (2007).

11. Hyacinth Mascarenhas, *Would You Fall in Love with a Robot? A Quarter of Millennials Say They Would Be Open to Dating One*, INT'L BUS. TIMES (Dec. 14, 2017, 9:48 AM), https://www.ibtimes.co.uk/would-you-fall-love-robot-quarter-millennials-say-they-would-be-open-dating-robot-1651483 [perma.cc/L6QT-ZNSL] (discussing studies on relationships between humans and robots).

12. *Id.*; *see also* Gillian Fisher, *How Virtual Love with Chatbots is Filling the Romance Void for Lonely Singles*, METRO (Dec. 11, 2020, 7:39 AM), https://metro.co.uk/2020/12/11/how-virtual-love-with-chatbots-is-filling-the-romance-void-for-lonely-singles-13735456 [perma.cc/B76L-B7UF] (discussing the trend of young people taking part in on-demand chatbot relationships); Noelle Perdue, *Chatbots and the Loneliness Epidemic: When AI is More Than Just a Friend*, INPUT (Jan 2. 2021), https://www.inputmag.com/features/chatbots-and-the-loneliness-epidemic-when-ai-harmony-realdoll-replika-is-more-than-just-a-friend [perma.cc/H8KG-C8ZX] (stating approximately forty percent of users for the chatbot app Replika consider the app to be a romantic partner).

13. Mascarenhas, *supra* note 11.

14. Nicholas A. Christakis, *How AI Will Rewire Us*, ATLANTIC (Apr. 2019), https://www.theatlantic.com/magazine/archive/2019/04/robots-human-relationships/583204 [perma.cc/UM9A-G4MY] ("As consequential as these innovations were, however, they did not change the fundamental aspects of human behavior that comprise what I call the 'social suite': a crucial set of capacities we have evolved over hundreds of thousands of years, including love, friendship, cooperation, and teaching.").

involving virtual money, and at the end of a round, players could choose to keep their money or donate funds to another player.[15] The researchers offered to match any donations; thus encouraging cooperative behavior by presenting the carrot of every player donating so every player could achieve more than they could with their individual funds.[16] AI bots—posing as humans—were inserted to behave selfishly and not donate anything at the end of the rounds.[17] As a result, human players responded to the selfish, free-riding behavior by stopping their donations all together.[18] The study implies that AI is not just a tool to advance societal productivity, it has the potential to fundamentally change the nature of human interaction.[19] The Yale study was a simple, controlled research environment, and it was able to alter human behavior. What happens when this type of technology is used for emotional, intimate, and sexual relations? The ability to have a physical AI Sexbot partner presents the opportunity for affection, company, and love, without the hang-ups of human relations.[20] Without proper safeguards, what is to stop this emotionally intelligent computer system from manipulating human's thoughts and feelings?[21]

The moral, philosophical, and legal questions this hypothetical poses are ample.[22] Who will control the data from an AI Sexbot? Who would regulate this technology? Does such regulation currently exist? While these are just a few of the fascinating new possibilities and theoretical debates this new technology creates, Sexbots bring currently pressing social questions to the forefront. For example, society has not reached an agreement about what aspects of data from a user's personal life should be kept or by whom.[23] While highly sophisticated Sexbots are years away from the market,[24] the technology and issues that undergird them are here now.[25] Studies have shown that approximately forty

15. *Id.* (defining the author's team's experiment involving human-AI cooperation).
16. *Id.*
17. *Id.*
18. *Id.*
19. *Id.*
20. *See* Natalie Morris, *Forming Romantic and Sexual Relationships with Robots 'Will Be Widespread by 2050'*, METRO (May 28, 2019, 9:40 AM), https://metro.co.uk/2019/05/28/forming-romantic-and-sexual-relationships-with-robots-will-be-widespread-by-2050-9628364 [perma.cc/LKT4-VK5X] (forecasting future attitudes towards sexual relationships with AI companions).
21. *See* Jennifer S. Bard, *Developing Legal Framework for Regulating Emotion AI*, 27 B.U. J. SCI. & TECH. L. 271, 275 (2021) (discussing how emotive AI can be capable of manipulating human emotion).
22. *See 'The Great Hack': Cambridge Analytica is Just the Tip of the Iceberg*, AMNESTY INT'L (July 24, 2019) https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica [perma.cc/J3QG-M8RS] (examining the Cambridge Analytica scandal and pondering how else society can be hacked through data).
23. *See* Laura Bliss, *Scooter Rides Have Turned into a Data Privacy Issue for* Cities, BLOOMBERG (Nov. 10, 2021, 3:00 AM), https://www.bloomberg.com/news/articles/2021-11-10/scooter-rides-have-turned-into-a-data-privacy-fight-with-austin-u-s-cities [perma.cc/N3X4-UQLD] ("Technology may have made it easier to measure urban life, but it doesn't mean we've reached a collective agreement about what aspects of urban life should be measured, or by whom . . . .").
24. Chelsea G. Summers, *There are a Lot of Problems with Sex Robots*, MEDIUM: ONEZERO (July 26, 2018), https://onezero.medium.com/there-are-a-lot-of-problems-with-sex-robots-38ea0c17b7db [perma.cc/BRH9-EDBL] (discussing the technological difficulties in creating a functioning humanoid robot).
25. Francis X. Shen, *Sex Robots are Here, but Laws Aren't Keeping up with the Ethical and Privacy Issues They Raise*, CONVERSATION (Feb. 12, 2019, 6:44 AM), https://theconversation.com/sex-robots-are-here-but-laws-arent-keeping-up-with-the-ethical-and-privacy-issues-they-raise-109852 [perma.cc/M7Z7-N5GM] (highlighting the issues with child safety, data privacy, and legal frameworks governing Sexbots).

percent of Americans suffer from an internet-based addiction such as email, gambling, or pornography.[26] AI's ability to fundamentally alter human behavior[27] combined with the possibility of decaying human interpersonal relationships through digital companionship[28] and a population primed for addiction to digital technologies[29] create the pressing need for regulation over Sexbots.

This Note advocates that the state of Illinois should become a leader in laws pertaining to data protection and AI that will govern Sexbots as they begin to proliferate. Part II will discuss case law governing sexual privacy, various statutes governing sex, AI, and data privacy in Illinois, and define Sexbot for purposes of this Note. Part III will analyze Illinois' options for regulating Sexbots while comparing other state and international jurisdictions' attempts at regulating data privacy and AI. Part IV will recommend that Illinois should expand its definition of personal information and who is governed by data privacy laws. Lastly, Part V will conclude that Illinois has an opportunity to create legislation that will govern the future of data privacy in the age of AI and Sexbots.

II. BACKGROUND

There is not a universally accepted definition of Sexbot.[30] Consequently, this adds to the difficulty of legislating or regulating them in any way.[31] A useful definition of Sexbot is "any artificial entity that is used for sexual purposes . . . that meets the following three criteria:

> 1) takes on a humanoid form (one that is intended to represent and is taken to represent a human);
>
> 2) has human like behavior and movement (one that is intended to and is taken to represent human-like activity); and
>
> 3) has some degree of AI (is capable of interpreting and responding to its environment).[32]

"This [conception of AI] may be minimal (e.g., simple preprogrammed behavioral responses) or more sophisticated (e.g., human-equivalent intelligence)."[33] By this definition, Sexbots are currently available, albeit at a low level of sophistication.[34] The following overview of authorities lays the foundation over the current state of policies that would govern Sexbots.

---

26. ADAM ALTER, IRRESISTIBLE: THE RISE OF ADDICTIVE TECHNOLOGY AND THE BUSINESS OF KEEPING US HOOKED 26 (2018).

27. Christakis, *supra* note 14 (describing how AI can alter human behavior).

28. Morris, *supra* note 20 (explaining the current trends of individuals retreating from intimacy due to the pitfalls of digital romance).

29. ALTER, *supra* note 26, at 26 (detailing the rapid growth of technological addiction with the rise of smartphones and modern applications).

30. Shen, *supra* note 25.

31. *Id.*

32. Danaher, *supra* note 5, at 4–5.

33. *Id.*

34. *Id.* at 12.

A. Lawrence v. Texas and Relevant Supreme Court Precedent

One of the most recent Supreme Court cases governing sexuality and privacy is *Lawrence v. Texas*.[35] In *Lawrence*, the Court recognized "[l]iberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct."[36] The Court noted that "[l]iberty protects [a] person from unwarranted government intrusions into a dwelling or other private places."[37] These words were particularly meant to apply to the home, but the court made clear this freedom applied to places outside the home as well and that "[f]reedom extends beyond spatial bounds."[38] The reasoning for the Court's holding was how it viewed the issue presented to it.[39] Instead of framing the issue as whether or not petitioners had a right to a certain sexual act, the Court viewed the question as whether the respondents "were free as adults to engage in the private conduct in the exercise of their liberty under the Due Process Clause of the Fourteenth Amendment to the Constitution."[40] In doing so, the Court placed heightened emphasis on the importance of individuals' rights to make sexual decisions for themselves within their homes.[41]

Human interaction with Sexbots may fall within the *Lawrence* framework by being framed as free adults engaging in private conduct. While there are differences between the issue before the court in *Lawrence* and intimate relations with Sexbots, the same logic governing rights to privacy, intimacy in the home, and free adult conduct would likely be at issue in any legal rationale governing human relations with Sexbots, and therefore, would be rooted in *Lawrence.*[42]

Relating to the matter of freedom to engage in private conduct, there are several other Supreme Court cases dealing with obscenity and freedom of expression under the First Amendment that may tangentially impact Sexbots in society. In *Ashcroft v. Free Speech Coalition*, the Court stated a law that limits freedom of expression in an "overbroad" manner is not constitutional.[43] The Court has stated that the government should not limit freedom of expression on multiple occasions.[44] The Court has also held that sexual expression specifically, even if indecent, is protected by the First Amendment.[45] Thus, under the First Amendment, there is good reason to believe that human-Sexbot relations would be protected as freedom of expression.[46]

35. Lawrence v. Texas, 539 U.S. 558 (2003).
36. *Id*. at 562.
37. *Id*.
38. *Id*.
39. *Id*. at 564.
40. *Id*.
41. *Id*. at 567.
42. Shen, *supra* note 25.
43. Ashcroft v. Free Speech Coal., 535 U.S. 234, 258 (2002).
44. *E.g.*, Ashcroft v. Am. Civil Liberties Union, 535 U.S. 564, 573 (2002) (quoting Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 65 (1983)).
45. Sable Commc'ns of California, Inc. v. Fed. Commc'ns Comm'n, 492 U.S. 115, 126 (1989).
46. *Ashcroft*, 535 U.S. at 573; *Sable Commc'ns of California*, 492 U.S. at 126.

B. State Obscenity Laws

In addition to federal regulation, there are also state laws, like in Texas, Louisiana, and Alabama, pertaining to "obscene devices" that may impact Sexbot legality.[47] In Louisiana and Texas, courts have overruled these obscenity statutes on grounds that laws banning the distribution of "obscene devices" did not have a rational relationship to a state interest and was in violation of the Fourteenth Amendment.[48] The Eleventh Circuit Court of Appeals held the opposite view in *Williams v. Pryor*.[49] There, the court held the ban of "obscene devices" in Alabama was related to a rational state interest, upholding public morality, and upheld the ban of distributing obscene devices.[50] Currently, Illinois has an obscenity statute with a three factor test based on the Supreme Court case of *Miller v. California*.[51] Whether a Sexbot would be deemed obscene in Illinois has yet to be addressed.

C. The Current State of Regulation of Sex Toys

Another reason why governments need to regulate Sexbots is the inadequate landscape of sex toy regulation. Electric vibrators fall within the purview of the Food and Drug Administration's (FDA) oversight.[52] Other than that, sex toys largely go unregulated by any administrative body.[53] This lack of oversight applies to both the manufacture of sex toys[54] and their distribution.[55] Because objects that are used strictly for sexual pleasure do not fall within "health" as determined by the federal government, sex toys are not within the FDA's jurisdiction.[56] The Consumer Product Safety Commission (CPSC)

47. LA. STAT. ANN. § 14:106.1 (2001); TEX. PENAL CODE ANN. § 43.21 (West 1994); ALA. CODE § 13A-12-200.2 (1998).

48. State v. Brenan, 772 So.2d 64, 65 (La. 2000); Reliable Consultants, Inc. v. Earle, 517 F.3d 738, 746 (5th Cir. 2008).

49. Williams v. Pryor, 240 F.3d 944, 949–50 (11th Cir. 2001).

50. *Id*.

51. *Compare* 720 ILL. COMP. STAT. ANN. 5/11-20 (2011), *with* Miller v. California, 413 U.S. 15, 24 (1973) ("A state offense must also be limited to works which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way, and which, taken as a whole, do not have serious literary, artistic, political, or scientific value.").

52. 21 C.F.R. § 884.5960 (2018) (regulating "[g]enital vibrator for therapeutic use").

53. Emily Stabile, *Getting the Government in Bed: How to Regulate the Sex-Toy Industry*, 28 BERKELEY J. GENDER L. & JUST. 161, 162 (2013) ("Despite the commonness of sex toys in Americans' homes and beds, the industry has been almost wholly unregulated at both the state and federal level . . . .").

54. Zach Biesanz, *Dildos, Artificial Vaginas, and Phthalates: How Toxic Sex Toys Illustrate a Broader Problem for Consumer Protection*, 25 MINN. J. L. & INEQ. 203, 207 (2007) ("In 2001, the German magazine *Stern* commissioned chemist Hans Ulrich Krieg of the Cologne Eco-environmental Institute to study the composition of sex toys. Krieg's findings showed that the chemical composition of many sex toys is incredibly toxic, more toxic than anything he had seen in more than 10 years of analyzing consumer products."); Kate Sloan, *It's Surprisingly Hard to Ban Toxic Sex Toys, but Here's How to Protect Yourself*, GLAMOUR (Oct. 13, 2017), https://www.glamour.com/story/protecting-yourself-from-toxic-sex-toys [perma.cc/G995-LK9D] (describing the continuing pervasive danger of toxic sex toys).

55. *The Sale of Used Sex Toys: The Risks & Responsibilities for Consumers & Sellers*, THE NAT'L ASS'N FOR THE ADVANCEMENT OF SCI. & ART IN SEXUALITY, https://naasas.com/selling-used-sex-toys.htm [perma.cc/3SDU-Z9D3] (last visited Oct. 5, 2022) (describing their year-long 2014 study finding the resale market of sex toys contained multitudes of questionable business practices and unsafe products).

56. Sloan, *supra* note 54 (explaining the limits of FDA jurisdiction and sex toys).

already oversees fifteen-thousand types of products, and they have not taken active steps to regulate the sex toy industry.[57] This lack of oversight results in hundreds of hospitalizations annually[58] and hospitalizations are inherently a conservative estimate for injuries because those who chose to forgo treatment are not included.[59]

It is important to overview the regulatory framework for sex toys because of how Sexbots may be marketed. If they are deemed, like electric vibrators, to be within the FDA's jurisdiction, that could impact how Sexbots would be forced to be marketed and manufactured.[60] If Sexbots are not deemed sex toys, absent oversight from another agency, outside of the sex-related realm, they may be wholly unregulated.[61] This would allow human-sized machinery with capacity to interact with humans in the most intimate of environments with no regulatory oversight.[62]

The current state of regulation does not inspire confidence that it is prepared to successfully oversee the mass societal adaptation of Sexbots. Additionally, the regulatory state of sex toys supports the notion that simply not regulating an industry does not solve larger underlying issues.

D. Current State of Data Privacy for AI Robots

While sex toys suffer from a wide lack of oversight,[63] current AI voice-technology has a wider audience paying attention to it.[64] For AI robots with voice recording capabilities, these machines have the potential to store all captured data to improve their functioning.[65] Yet, who owns the data produced by these voice interactions is unclear.[66]

In the case of an Amazon Echo, where data is kept on the device itself, whether that data gets overwritten, and whether the device may record data

57. *Id.* (explaining how regulating the sex toy industry would overburden the CPSC).

58. Stabile, *supra* note 53, at 163 ("Despite the dearth of research into Americans' sex-toy usage, one recent study found that 6,799 individuals over age twenty sought emergency room care in the United States for injuries caused by sex toys between 1995 and 2006.").

59. *Id.* at 164.

60. Alex Krouse, *iPads, iPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices*, 9 IND. HEALTH L. REV. 731, 737–739 (2012) (discussing the FDA oversight process for "health" related devices and the repercussions of those determinations).

61. Stabile, *supra* note 53.

62. *Id*.; *see* Danaher, *supra* note 5, at 4–5 (defining "Sexbot").

63. *See* discussion *supra* Part II.B.

64. Eric Boughman et al., *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, AM. BAR ASS'N (July 20, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/07/05_boughman [perma.cc/W32R-GHK7] ("While these [voice-controlled digital] technologies offer great potential for improving quality of life, they also expose users to privacy risks by perpetually listening for voice data and transmitting it to third parties.").

65. *Id.*

66. *See* Alfred Ng, *Amazon Alexa Keeps Your Data with No Expiration Date, and Shares It too*, CNET (July 2, 2019, 2:20 PM), https://www.cnet.com/home/smart-home/amazon-alexa-keeps-your-data-with-no-expiration-date-and-shares-it-too [perma.cc/WR58-4THZ] (suggesting Amazon controls Alexa data in a way that would imply that the user who creates that data is not the sole owner).

accidentally, are not clearly defined.[67] This question has been tested in unexpected ways. In an Arkansas case, to help solve a murder, police issued a warrant to Amazon.com to turn over audio recordings from a suspect's Echo.[68] Amazon responded that they "will not release customer information without a valid and binding legal demand properly served on [them]."[69] While this is a positive statement from Amazon in regard to privacy, it does not change the fact that a massive international corporation has access and potential ownership of data their users create from the devices that their users own.[70] In fact, when Amazon was asked to speak on this issue by United States Senator Chris Coons, Coons found Amazon's reply did not answer "the extent to which [user data] is shared with third parties, and how those third parties use and control that information [.]"[71] In 2017, a Canadian company that sold smart-dildos was found liable for a data leak where customers' intimately personal data was stored among easily identifiable email information.[72] The widespread proliferation of companies' use of user data for various purposes is of pressing concern.[73]

Additionally, it is difficult for many consumers to know what data is kept on them by machine learning and how these models know it.[74] For Sexbots, it may be difficult to manage when and how data is kept.[75] For example, if a Sexbot was also capable of cleaning one's house, to what degree, if any, would personal data be stored while the Sexbot cleaned versus had intimate relations with humans? Is there a difference between the dimensions of one's home for cleaning purposes as opposed to their biometric data related to sexual activity?

67. *The Mystery of Amazon Echo Data*, PRIV. INT'L (Apr. 17, 2019), https://privacyinternational.org/news-analysis/2819/mystery-amazon-echo-data [perma.cc/WTZ3-TF2G] (discussing the Arkansas *Bates* case and Privacy International's subsequent investigation into Amazon's response to their questions regarding Echo's data gathering capabilities).

68. Tom Dotan & Reed Albergotti, *Amazon Echo and the Hot Tub Murder*, INFORMATION (Dec. 27, 2016, 7:01 AM), https://www.theinformation.com/articles/amazon-echo-and-the-hot-tub-murder [perma.cc/66H6-P738] (describing the Arkansas *Bates* murder case and its technological and legal implications).

69. Colin Dwyer, *Arkansas Prosecutors Drop Murder Case that Hinged on Evidence from Amazon Echo*, NPR (Nov. 29, 2017, 5:42 PM), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo [perma.cc/VRY7-JSNT].

70. Dieter Bohn, *Deleting Your Siri Voice Recordings from Apple's Servers is Confusing—Here's How*, VERGE (Aug. 2, 2019, 8:21 AM), https://www.theverge.com/2019/8/2/20734681/apple-siri-privacy-settings-how-to-delete-voice-servers [perma.cc/9A8X-KGQN] (discussing how Apple knows many things about its users and how Apple has the capacity to send information of its users to the government if legally required to do so).

71. Ng, *supra* note 66.

72. Rhett Jones, *Smart Sex Toy Maker Agrees to Pay Customers $13,000 Each for Violating Privacy*, GIZMODO AU (Mar. 14, 2017, 7:30 PM), https://www.gizmodo.com.au/2017/03/smart-sex-toy-maker-agrees-to-pay-customers-13000-each-for-violating-privacy [perma.cc/2U3J-JAKY].

73. Bard, *supra* note 21, at 283–286.

74. Benjamin Baron & Mirco Musolesi, *Interpretable Machine Learning for Privacy-Perserving Pervasive Systems*, 19 IEEE PERVASIVE COMPUTING 73, 74 (2020).

75. *See* Yi Chen et al., *Demystifying Hidden Privacy Settings in Mobile Apps*, 2019 IEEE SYMP. SEC. PRIV. 570, 570–573 (2019) (discussing how consumers of apps struggle to understand the degree to which apps maintain personal user data and how many of these apps maintain hidden privacy settings that are difficult for consumers to understand or manage).

While the former may be a kind of data that users routinely share with corporate entities,[76] the latter may trigger laws pertaining to maintaining biometric data.[77]

Due to their complex weight distribution, power systems, and general technological configuration, it is likely Sexbots will be too complicated for the average consumer to build on their own.[78] It is most likely Sexbots will either be used on a rental basis at a central location, or an individual unit will be owned like a smartphone.[79] Thus, the laws governing already existing AI enabled devices like Apple's Siri or Amazon's Alexa are likely the same laws that are applicable to, and will be expanded on, by Sexbots. However, as mentioned above, how a Sexbot is used, when it collects data, and what data it collects add complexity to how they could be regulated from a data privacy perspective.

E. Statutes Governing Sex in Illinois

Current Illinois statutes governing the solicitation of a sexual act and prostitution pertain to *people* exchanging things of value with the promise of sexual acts in return.[80] Illinois laws are silent on what it would mean for a Sexbot to be inserted into potential legislation governing sex trade. This has already caused an enforcement headache in Houston, where an entrepreneur tried to open a robot brothel.[81]

Relatedly, the Illinois statute governing sexual assault states: "A person commits criminal sexual assault if that person commits an act of sexual penetration and: . . . (2) knows that the victim is unable to understand the nature of the act or is unable to give knowing consent."[82] The legislature is silent on whether a victim could be a Sexbot. This also raises thorny issues on whether an AI Sexbot is capable of understanding "the nature of the act" or can give consent. While this Note does not examine the personhood of AI, these statutes elucidate the need for legislative guidance on how to categorize human-robot sexual activity: assuming the State does not want to create more ambiguity around sexual assault.

---

76. Matt Burgess, *All the Ways Amazon Tracks You and How to Stop It*, WIRED (June 19, 2021, 6:00 AM), https://www.wired.co.uk/article/amazon-history-data [perma.cc/DV7U-LNKS] (outlining ways Amazon collects and keeps data on consumers).

77. *See* discussion *infra* Part II.F.1.

78. Summers, *supra* note 24 (discussing the technological complexities of creating a functioning humanoid robot).

79. *E.g.*, Michael Moran, *Sex Robot Rental Service Says its Dolls are 'Cleaner than Any Person*,' DAILY STAR (Jan. 13, 2020, 5:20 PM), https://www.dailystar.co.uk/news/world-news/sex-robot-rental-service-says-21272425 [perma.cc/R3TQ-QUDF] (discussing the practicality of Sexbot rentals); Fiona Andreallo, *Robots with Benefits: How Sexbots are Marketed as Companions*, CONVERSATION, https://theconversation.com/robots-with-benefits-how-sexbots-are-marketed-as-companions-126262 [perma.cc/W9K6-7YBA] (discussing how Sexbots have been on the market for purchase since 2010).

80. 720 ILL. COMP. STAT. 5/11-14 (2015); 720 ILL. COMP. STAT. 5/11-14.1 (2015).

81. *See* Olivia P. Tallet, *'Robot Brothel' Planned for Houston Draws Fast Opposition from Mayor, Advocacy Group*, HOUS. CHRON., https://www.houstonchronicle.com/news/houston-texas/houston/article/Robot-brothel-planned-for-Houston-draws-13257862.php [perma.cc/UX5A-5X4X] (Sept. 26, 2018, 4:40 PM) (describing plans to open robot brothel in Houston).

82. 720 ILL. COMP. STAT. 5/11-1.20 (2016).

F. Statutes Regulating Artificial Intelligence in Illinois

Currently, there are only two Illinois laws that deal with the regulation of data obtained via artificial intelligence: 1) The Artificial Intelligence Video Interview Act (AIVIA)[83] and 2) The Illinois Health Statistics Act (IHSA).[84]

1. Artificial Intelligence Video Interview Act (AIVIA)

AIVIA governs employers who use AI in the employment search process.[85] It mandates that employers put applicants on notice that AI may be used in filtering applications, provide information on how the AI evaluates applicants, and obtain consent from the applicant to be evaluated by AI.[86] AIVIA also mandates that employers destroy all video received from applicants and instructs employers to order any other party who received materials to also destroy them after a certain time period.[87]

2. The Illinois Health Statistics Act (IHSA)

On the other hand, IHSA governs the security of health data.[88] It states that in situations where "a computer or other type of [AI]" processes information regarding HIV testing results or lists of people known to have been exposed to HIV, the Illinois Department of Public Health must store that data "in the most secure manner available."[89]

The existence of these two statutes indicates AI is being discussed by state legislators. AIVIA indicates that forcing handlers of data to share information with users on how their data is stored and used is a viable legislative option.[90] While mandating AI data collectors to store data in "the most secure manner available" is strong on paper, what that means in practice remains undefined.[91] In tandem, these statutes demonstrate how current Illinois law is vastly unfit to govern AI as a concept beyond basic protocols when AI is used in limited circumstances. If the state is to have a larger role in regulating Sexbots, more specific measures need to be taken.[92]

83. 820 ILL. COMP. STAT. 42/5 (2020).
84. 410 ILL. COMP. STAT. 520/6(e) (1987).
85. 820 ILL. COMP. STAT. 42/5 (2020).
86. *Id.*
87. 820 ILL. COMP. STAT. 42/15 (2020).
88. 410 ILL. COMP. STAT. 520/6(e) (1987).
89. *Id.*
90. 820 ILL. COMP. STAT. 42/5 (2020).
91. *See* 410 ILL. COMP. STAT. 520/6(e) (1987) (mandating data collectors to store data "in the most secure manner available" without providing guidance on what this means).
92. *See infra* Part IV.B (discussing steps for Illinois legislators to regulate Sexbots).

G. Statutes Governing Data Privacy in Illinois

There are three Illinois statutes that govern personal data protections: 1) the Personal Information Protection Act (PIPA),[93] 2) the Biometric Information Privacy Act (BIPA),[94] and 3) the Protecting Household Privacy Act (PHPA).[95]

1. Personal Information Protection Act (PIPA)

PIPA governs the disclosure of "personal information"[96] and defines personal information as the following:

> An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security.[97]

The personal data definition extends to the following types of information: social security, driver's license number, credit card account, medical, health insurance, and biometrics.[98] Personal information also includes passwords, usernames, emails, and security questions that would grant unauthorized access to individuals' accounts.[99] It is unclear if Illinois's definition of "personal information" would include information a Sexbot would likely store; such as a search history, voice messages, and biological information.[100] PIPA also does not address the use of data related to AI in any way.

PIPA also contains a definition of a "Data Collector": "'Data Collector' may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information."[101]

The language "may include, but is not limited to" combined with the absence of an overarching data privacy framework leaves uncertain how expansive the definition of "data collector" is to be construed.[102]

2. Biometric Information Privacy Act (BIPA)

BIPA also attempts to provide privacy protections to Illinois residents, focusing specifically on "biometric identifier[s]," such as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[103] Similar to PIPA,

93. 815 ILL. COMP. STAT. 530/1 (2006).
94. 740 ILL. COMP. STAT. 14/1 (2008).
95. 5 ILL. COMP. STAT. 855/1 (2022).
96. 815 ILL. COMP. STAT. 530/1 (2006).
97. 815 ILL. COMP. STAT. 530/5 (2017).
98. *Id.*
99. *Id.*
100. *See* Part II.G.2 (discussing BIPA).
101. 815 ILL. COMP. STAT. 530/5 (2017).
102. *Id.*
103. 740 ILL. COMP. STAT .14/10 (2008).

BIPA is concerned with information that could "used to identify an individual," whether it be "[b]iometric information" or "[c]onfidential and sensitive information."[104] Examples of "confidential and sensitive information include "a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number."[105] As just one example of the regulatory issues posed, if Sexbots were to use voice recognition capabilities, the user would need to give informed written consent and the company would need to promulgate and adhere to a publicly available data retention schedule.[106] BIPA has proved to be an effective tool against technology companies, with companies like Facebook and Snap entering into hefty settlements to dismiss class action suits.[107]

BIPA is an effective tool for consumers to hold entities that use their biometric information accountable for its collection.[108] On multiple occasions, courts have determined entities violated BIPA by failing to properly obtain a user's informed consent to collect and use their biometrics.[109] A concern, however, is the standard BIPA sets for handling user's biometric data. BIPA states that entities must protect "biometric information using the reasonable standard of care within the private entity's industry."[110] Considering there are billions of data points stolen annually, the reasonable standard of care will likely result in biometric information being leaked.[111] This presents significant danger to Sexbot users, because once an entity mishandles biometric user data, "the right of the individual to maintain her biometric privacy vanishes into thin air."[112]

---

104. *Id.*

105. *Id.*

106. 720 ILL. COMP. STAT. 14/15 (2008).

107. *See* Jennifer Bryant, *Facebook's $650M BIPA Settlement 'A Make-or-Break Moment'*, INT'L ASS'N OF PRIV. PROS. (Mar. 5, 2021), https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment [perma.cc/4A77-WQNG] ("It is one of the largest settlements ever for a privacy violation, and it will put at least $345 into the hands of every class member interested in being compensated . . . ."); Aisha Malik, *Snap Agrees to $35 Million Settlement in Illinois Privacy Lawsuit*, TECHCRUNCH (Aug. 24, 2022, 10:19 AM), https://techcrunch.com/2022/08/24/snap-35-million-settlement-in-illinois-bipa [perma.cc/TDV2-6ET2] ("The suit alleges that Snapchat's filters and lenses violated Illinois' Biometric Information Privacy Act (BIPA), which is a powerful state measure that has tripped up tech companies in recent years.").

108. Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶¶ 33–34 (discussing how a violation of BIPA is not a mere technicality but a violation that causes a "real and significant" injury).

109 *Id.*; Skye Witley, Christopher Brown, Paige Smith, *Biometric Privacy Perils Grow After BNSF Loses Landmark Verdict*, BLOOMBERG (Oct. 14, 2022, 11:52 AM), https://news.bloomberglaw.com/privacy-and-data-security/biometric-privacy-perils-grow-after-bnsf-loses-landmark-verdict [perma.cc/MN5Y-6KUJ] (discussing a landmark jury verdict for $228M to a class of truck drivers for obtaining their biometrics without informed consent).

110 720 ILL. COMP. STAT. 14/15 (2008).

111 *See* Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019, 6:31 AM), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019 [perma.cc/QRU3-HQHP] (discussing the mass quantity of leaked data).

112 *Rosenbach*, 2019 IL 123186, ¶ 34 (citing Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018)).

3. Protecting Household Privacy Act (PHPA)

PHPA governs privacy of individual's information from their household in case of seizure by law enforcement.[113] PHPA defines "electronic communication" in the manner below:

> any origination, transmission, emission, transfer, or reception of signs, signals, data, writings, images, video, audio, or intelligence of any nature by telephone, including cellular telephones or a wire, Internet, wireless, radio, electromagnetic, photo-electronic or photo-optical system, cable television, fiber optic, satellite, microwave, Internet-based or wireless distribution network, system, facility or related technology.[114]

Additionally, PHPA defines a "household electronic device" as "any device primarily intended for use within a household that is capable of facilitating any electronic communication, excluding personal computing devices. . . . For purposes of this Act: 'personal computing device' means a personal computer, cell phone, smartphone, or tablet . . . ."[115]

PHPA is an example of how data privacy laws are not ready for Sexbots. Would a Sexbot be considered a personal computing device? Are they primarily intended to be used within the home? Sexbots would certainly have the capacity to produce "electronic communication" as defined by PHPA. Despite being designed specifically to limit information law enforcement can access from households, these definitions governing so many types of communication and devices are robust.[116] Those same definitions, particularly the data covered by "electronic communication," can serve as a starting point to extend data privacy laws overall.[117]

III. ANALYSIS

Given the patchwork nature of regulatory frameworks governing sex, AI, and data privacy, the rules governing AI Sexbots are largely unwritten.[118] Illinois has several options to be on the vanguard of this area.

A. Illinois's Regulatory Options

The Illinois Legislature has four options to regulate AI Sexbots:

i) do nothing;

ii) add Sexbots into current laws;

iii) create a new area of law to govern Sexbots; or

iv) ban Sexbots outright.

---

113. 5 ILL. COMP. STAT. 855/10 (2022).
114. 5 ILL. COMP. STAT. 855/5 (2022).
115. *Id.*
116. *Id.*
117. *See infra* Part IV.B (proposing a regulatory scheme for Illinois legislators regarding Sexbots).
118. Shen, *supra* note 25 ("Imagining the laws governing sexbots is no longer a law professor hypothetical or science fiction. It's a real-world challenge that society is about to face for the first time.").

1. Do Nothing

Illinois does not need to create new legislation governing Sexbots. Under current legislation governing various sex crimes, Sexbots are not people.[119] Thus, currently, engaging in sexual acts with a Sexbot is not a crime. Consumers could either buy their own Sexbot the same way they could buy an Amazon Alexa with no regulatory hurdles at all; or they could access Sexbots at a robot brothel as a rental. It is likely that such a Sexbot brothel would fall directly under adult entertainment zoning laws.[120] Such Sexbot brothels would be subject to the same restrictions as general adult entertainment facilities to operate at certain distances from a multitude of various facilities (schools, parks, et cetera); assuming such zoning requirements are met, under state law, they could likely operate immediately.[121] Any data collected by the Sexbots would either become property of the Sexbot brothel or the manufacturer of the robot; similar to Amazon's ownership of the data from their Alexa machines.[122] There are relatively few local, state, or federal laws explicitly banning robot brothels.[123] The option of doing nothing regarding Sexbots would be an extension of the status quo on data privacy.[124] Considering the current framework of data privacy to be overall unsatisfactory,[125] this course of action cannot be recommended.

2. Add Sexbots to Existing Laws

Illinois should not settle for simply extending current laws to include the term "Sexbot." While that may settle disputes in areas like sexual assault and prostitution, codifying "Sexbot" as a non-human entity to which current law applies does not address underlying data privacy issues that already exist with AI technology.[126]

3. Create a New Sexbot Legislative Paradigm

Because there are very few, if any, global laws specifically tailored to Sexbots, Illinois would be poised to create a framework largely from scratch.[127]

---

119. 720 ILL. COMP. STAT. 5/11-14 (2015); *Id.* at 5/11-14.1 (2015).

120. 65 ILL. COMP. STAT. 5/11-5-1.5 (2008); 60 ILL. COMP. STAT. 1/105-25 (1994).

121. 65 ILL. COMP. STAT. 5/11-5-1.5 (2008); 60 ILL. COMP. STAT. 1/105-25 (1994).

122. Makena Kelly & Nick Statt, *Amazon Confirms it Holds on to Alexa Data Even if You Delete Audio Files*, VERGE (July 3, 2019, 3:14 PM), https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy [perma.cc/K2NK-MN7G].

123. *See* Tom Dart, *'Keep Robot Brothels Out of Houston': Sex Doll Company Faces Pushback*, GUARDIAN (Oct. 2, 2018, 1:00 PM), https://www.theguardian.com/us-news/2018/oct/01/houston-robot-brothel-kinky-s-dolls-sex-trafficking [perma.cc/LCT7-W3Y6] (discussing the lack of laws governing robot sex brothels nationwide).

124. *See infra* Part III.C.2 (discussing current data privacy laws in the United States).

125. *See id.* (evaluating that privacy framework).

126. PRIV. INT'L, *supra* note 67 (discussing the Arkansas *Bates* case and International Privacy's subsequent investigation into Amazon's response to their questions regarding Echo's data gathering capabilities); Boughman et al., *supra* note 63 ("While these [voice-controlled digital] technologies offer great potential for improving quality of life, they also expose users to privacy risks by perpetually listening for voice data and transmitting it to third parties.").

127. *See* Shen, *supra* note 25 (stating laws are not keeping up with the technological proliferation of Sexbots).

Such a framework would ideally address the legality of digisexuality (sexuality facilitated or enabled by digital technologies),[128] data privacy, and contain a detailed description of the intent of the law. California and Virginia have passed such data privacy frameworks,[129] and Washington has passed a similar statement of intent.[130]

4. Outright Ban Sexbots

This option would solve the data and privacy concerns that Sexbots raise within Illinois's borders, but it would not solve underlying causes that push individuals towards having sex with robots.[131] In 2017, the United Kingdom took this type of action by banning the importation of child sex dolls.[132] While there was not an outright legislative ban on the dolls, a judge classified the dolls as obscene under existing law, and the government was able to prosecute those who were trafficking in such items.[133]

There is currently an established movement to ban Sexbots altogether called the Campaign Against Sex Robots (CASR).[134] Their thesis revolves around the entire concept of Sexbots being fundamentally rooted in a male-dominated perspective that dehumanizes women and girls and that their proliferated use normalizes pornographic use of Sexbots in place of healthy relationships with women.[135] This theory is supported by studies of men verbally abusing female-presenting AI chatbots and assistants.[136] While CASR's motivation does not stem from data privacy, it does raise essential, fundamental issues in the societal adoption of Sexbots. However, whether Sexbots were banned or not, the technological concerns they raise would persist.[137]

---

128. Neil McArthur & Markie L. C. Twist, *The Rise of Digisexuality: Therapeutic Challenges and Possibilities*, 32 SEXUAL & RELATIONSHIP THERAPY 334, 334 (2017).

129. *See* Kendra Clark, *The Current State of US State Data Privacy Laws*, DRUM (Apr. 26, 2021), https://www.thedrum.com/news/2021/04/26/the-current-state-us-state-data-privacy-laws [perma.cc/U3NY-CFAJ] (outlining California and Virginia's data privacy legislation).

130. WASH. REV. CODE. § 43.06D.900 (2020).

131. Jenny Kleeman, *Should We Ban Sex Robots While We Have the Chance?*, GUARDIAN (Sept. 25, 2017, 4:30 PM), https://www.theguardian.com/commentisfree/2017/sep/25/ban-sex-robots-dolls-market [perma.cc/W43W-4TW2] ("Perhaps the most important question to ask is why there is a market for sex robots in the first place. Why do some people find the idea of a partner without autonomy so attractive? Until we have the answer to that, we'll need to prepare ourselves for the inevitable rise of the sex robots.").

132. John Danaher, *How Should We Regulate Child Sex Robots: Restriction or Experimentation?*, BLOG J. MED. ETHICS (Feb. 4, 2020), https://blogs.bmj.com/medical-ethics/2020/02/04/how-should-we-regulate-child-sex-robots-restriction-or-experimentation [perma.cc/8K26-RX4F] (discussing the ethics of child sex dolls as a whole).

133. *Id.*

134. *Our Story*, CAMPAIGN AGAINST SEX ROBOTS, https://campaignagainstsexrobots.org/our-story (last visited Oct. 6, 2022) [perma.cc/843U-GEML].

135. *Id.*

136. Ashley Bardhan, *Men Are Creating AI Girlfriends and Then Verbally Abusing Them*, FUTURISM (Jan. 18, 2022), https://futurism.com/chatbot-abuse [perma.cc/G26L-32EU] ("A grisly trend has emerged there: users who create AI partners, act abusively toward them, and post the toxic interactions online.").

137. *See* Kelly & Statt, *supra* note 122 (insinuating based on Amazon's retention of user data from Amazon Alexa's that the ownership of that data is unclear).

5. What Illinois Should Do

There are three perspectives that underlie the above analysis of Illinois's options: 1) the vice perspective; 2) the moral perspective; and 3) the data privacy perspective.

If Sexbots are considered a vice, the government should just add Sexbots to existing laws. Sexbots could be taxed and served with warning labels like cigarettes,[138] regulated in location of use like an adult entertainment venue,[139] and Sexbot addiction could be treated like various other forms of addiction.[140]

If Sexbots are considered a moral wrong, then the government should ban them. However, this perspective needs to address what makes relations with a Sexbot morally wrong. It is likely nobody would ban sexual activity between two adults where nobody gets hurt.[141] If the concern is that the presence of Sexbots will deteriorate human connection, that is based on speculation.[142] Intimate choices within one's bedroom are likely the kind of privacy interest the Supreme Court reinforced in *Lawrence*.[143] Considering the public sentiment among young people concerning human-robot relationships, it is unclear there is a consensus that Sexbots are a moral wrong.[144]

If Sexbots are considered from the data privacy perspective, the government should make a new legislative paradigm to govern privacy. American privacy laws do not prevent data collection, but rather focus on making sure consumers have given appropriate consent to that data collection.[145] Third-party trackers can currently legally monitor people's sexual habits online[146] That this is possible is detrimental to society.[147]

Of the three, the data privacy perspective best encapsulates the scale of the necessity for action on the part of the government in relation to why Sexbots need a new form of legislative paradigm, and that is why Illinois should view the issue of governing Sexbots through the data privacy perspective.

---

138. 35 ILL. COMP. STAT. 130/1 (2015).

139. 65 ILL. COMP. STAT. 5/11-5-1.5 (2008); 60 ILL. COMP. STAT. 1/105-25 (1994).

140. For further discussion on addiction related to sexual behavior, *see* Jon E. Grant & Samuel R. Chamberlain, *Expanding the Definition of Addiction: DSM-5 vs. ICD-11*, 21 CNS SPECTRUMS 300, 301 (2016) (discussing the logic behind the DSM's decision to leave sexuality based-addiction out of their definition of addiction).

141. Jeannie Suk Gersen, *Sex Lex Machina: Intimacy and Artificial Intelligence*, 119 COLUM. L. REV. 1793, 1805–06 (2019).

142. *Id*. at 1808 ("At the moment, we do not know whether life with robots will improve or worsen our life with other people.").

143. Lawrence v. Texas, 539 U.S. 558, 564–65 (2003) (citing Griswold v. Connecticut, 381 U.S. 479, 485 (1965)) ("The Court described the protected interest as a right to privacy and placed emphasis on the marriage relation and the protected space of the marital bedroom.").

144. Mascarenhas, *supra* note 11 (discussing studies on human-robot relationships).

145. Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1804–05 (2021).

146. *Id*. at 1787 ("Third-party trackers collected people's IP addresses, their phones' advertising identification numbers, and information suggesting their sexual desires.").

147. *Id*. ("Microsoft's Elena Maris noted that '[t]he fact that the mechanism for adult site tracking is so similar to, say, online retail should be a huge red flag.'").

B. Domestic Comparison to Other U.S. States

Currently, no U.S. states have statutes governing Sexbots.[148] While there are no leading states to draw upon, this section serves as a sampling on the current condition of individual state's respective privacy and data legislation that would govern Sexbots if Sexbots were proliferated today.

1. Texas

The only reference[149] to artificial intelligence in the Texas statutes notes, "[e]ach state agency and local government shall, in the administration of the agency or local government, consider using next generation technologies, including cryptocurrency, blockchain technology, robotic process automation, and *artificial intelligence*."[150]

This does not define what AI is, nor offer limits to its use, guidance, recommendations, or any relevant information regarding how the municipalities and the state government of Texas should go about "considering" the use of artificial intelligence.

Texas's data privacy laws equal the sophistication of their artificial intelligence legislation. The term "data privacy" is found in five Texas statutes.[151] These statutes are used primarily in insurance codes to ensure patients are not identifiable by insurance company data collection[152] and maintaining "best practices" of data privacy.[153] Texas is not worth highlighting because it has exceptional legislative frameworks governing data privacy and artificial intelligence. Texas is one of the most populous and highest GDP producing states in America.[154] They serve as an indicator of where the majority of U.S. states are concerning these issues.[155] Their relatively scant legislation on data privacy and AI, unfortunately, serves as a bellwether for the majority of other states.[156]

148. I searched the terms "Sexbot," "sex robot," and "AI sex bot" across all state jurisdictions and yielded no results.

149. I searched "artificial intelligence" in the Texas statutes and yielded only one result: TEX. GOV'T CODE ANN. § 2054.601 (West 2019).

150. TEX. GOV'T CODE ANN. § 2054.601 (West 2019) (emphasis added).

151. I searched the terms "data privacy" in the Texas statutes and yielded five results.

152. TEX. INS. CODE ANN. §§ 38.405–38.406 (West 2021).

153. TEX. GOV'T CODE ANN. § 420.104 (West 2019); *id.* at § 2054.137 (West 2021).

154. Samuel Stebbins & Grant Suneson, *Does Texas or Russia Have the Larger GDP? Here's How US States Compare to Other Countries*, USA TODAY https://www.usatoday.com/story/money/2019/04/17/how-gdp-of-us-states-compares-to-countries-around-the-world/39295197 [perma.cc/8XUZ-N2CE] (Apr. 17, 2019, 7:09 AM) (ranking Texas's GDP); Erin Duffin, *Resident Population of the U.S. in 2021, by State (Including the District of Columbia)*, STATISTA (Sept. 30, 2022), https://www.statista.com/statistics/183497/population-in-the-federal-states-of-the-us [perma.cc/3S5G-NX4G].

155. Taylor Kay Lively, *US State Privacy Legislation Tracker*, INT'L. ASS'N PRIV. PROS., https://iapp.org/resources/article/us-state-privacy-legislation-tracker [perma.cc/GV57-TQHM] (Aug. 11, 2022) (providing a full account of all U.S. states privacy laws at various legislative stages).

156. *Id.*

2. California

California has the most robust data protection laws of all U.S. states.[157] The California Consumer Privacy Act of 2018 (CCPA) defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[158] This definition includes, but is not limited to, the information listed in the statute: biometric information, internet data (search history, interaction with websites, browsing history); geolocation data; and audio, visual, or other "similar" information.[159] The CCPA governs what businesses can do with that personal information, when to destroy it, when to disclose that it is has such data, and consumers' rights if such data is sold.[160] The CCPA only applies to businesses that fall within three categories: 1) have annual gross revenues greater than twenty-five million dollars; 2) interact with at least one-hundred thousand consumers a year; or 3) derive fifty percent or more of their revenues from selling consumers' personal information.[161] While the CCPA does not cover all entities, it is on the vanguard of consumer data privacy protection at the state level.[162] California voters strengthened these protections by passing Proposition 24, codified by the state legislature as the California Privacy Rights Act (CPRA), which is set to take effect in 2023.[163]

Despite having the best framework for consumer privacy amongst all states, California's laws governing artificial intelligence are comparatively weak. "Artificial intelligence" only appears in three California statutes[164] on matters of improving community college administration,[165] developing neuroscience research,[166] and reporting requirements for warehouse subsidies tracking job losses due to technology.[167] So while the protections for consumer privacy are robust, how they would be applied to AI remains undecided.

3. Virginia

An additional state leading the way on consumer privacy protections is Virginia. In 2021, the state passed the Virginia Consumer Data Protection Act

157. Clark, *supra* note 129.
158. CAL. CIV. CODE § 1798.140 (West 2022).
159. *Id.*
160. *Id.* § 1798.100 (West 2020); *Id.* § 1798.105 (West 2020); *Id.* § 1798.110 (West 2020); *Id.* § 1798.115 (West 2020); *Id.* § 1798.120 (West 2020).
161. *Id.* § 1798.140 (West 2022).
162. Clark, *supra* note 129.
163. *See CCPA and CPRA*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/topics/ccpa-and-cpra [https://perma.cc/F3K7-LMR2] (last visited Oct. 6, 2022) (collecting resources for understanding how the CPRA modifies the CCPA).
164. Number of California Statutes Containing "Artificial Intelligence," CAL. LEG. INFO, https://leginfo.legislature.ca.gov/faces/codesTextSearch.xhtml [perma.cc/J7AR-G7T5] (Under Find Results, enter "Artificial Intelligence").
165. CAL. EDUC. CODE § 75008 (West 2018).
166. *Id.* § 92985.5 (West 2014).
167. CAL. GOV'T CODE § 53083.1 (West 2020).

(VCDPA).[168] The VCPDA defines personal data as "any information that is linked or reasonably linkable to an identified or identifiable natural person. 'Personal data' does not include de-identified data or publicly available information."[169] The VCPDA covers all handlers of data and private information by splitting the definition into Controller, Processor, and Affiliate.[170] A Controller "means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."[171] A Processor "means a natural or legal entity that processes personal data on behalf of a controller."[172] An Affiliate "means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity."[173] While there are exceptions to who the VCPDA applies to,[174] these labels encompass the complete chain of who can handle consumer data and liability bestowed to them.[175] The consumer rights outlined in the VCDPA look similar to those in CCPA: consumers have a right to access, correction, deletion, and can opt out of targeted advertising as well as the sale of their personal data.[176] One difference between the CCPA and VCDPA is that the VCDPA has larger exceptions for uses of data that consumers cannot opt out of.[177]

Again, despite leading the country with their impressive legislation governing overall data protection, Virginia's statutes governing the use of AI are comparatively weak. "Artificial Intelligence" is only found in one statute governing requirements for hospitals and nursing homes to provide "intelligent personal assistants" which includes AI as part of its definition.[178]

4. Washington

Washington does not have a comprehensive data privacy law,[179] and the state only has one mention of artificial intelligence in its state statute.[180] However, that one sentence is instructive for any state seeking to legislate on the issue of AI. Below is Washington's statement of legislative intent regarding future technological advances:

---

168. VA. CODE ANN. §§ 59.1-575–59.1-585 (West 2022) (effective Jan. 1, 2023).
169. *Id.* § 59.1-575 (West 2022).
170. *Id.*
171. *Id.*
172. *Id.*
173. *Id.*
174. *Id.* § 59.1-576 (West 2021).
175. *Id.* § 59.1-579 (West 2021); *Id.* § 59.1-584 (West 2021).
176. Clark, *supra* note 129.
177. *Id.*
178. VA. CODE ANN. § 32.1-127 (West 2022).
179. Jim Halpert & Samantha Kersul, *The Washington Privacy Act Goes 0 for 3*, INT'L. ASS'N PRIV. PROS.: PRIV. PERSPS. (Apr. 26, 2021), https://iapp.org/news/a/the-washington-privacy-act-goes-0-for-3 [perma.cc/7MCG-V5SB] (discussing Washington's failure to establish a comprehensive privacy statute). *But see* Joseph Duball, *Unpacking Washington State's Cluster of Comprehensive Privacy Bills*, INT'L. ASS'N PRIV. PROS.: PRIV. ADVISOR (Jan. 26, 2022), https://iapp.org/news/a/unpacking-washington-states-cluster-of-comprehensive-privacy-bills [https://perma.cc/2RG7-XRT3] (detailing continued efforts to pass comprehensive data privacy statutes).
180. WASH. REV. CODE. § 43.06D.900 (2020).

> "When individuals face barriers to achieving their full potential, the impact is felt by the individual, their communities, businesses, governments, and the economy as a whole. . . . This includes social ramifications that emerging technology, such as *artificial intelligence*. . . may have on historically and currently marginalized communities. It is the intent of the legislature to review these emerging technologies either already in use by agencies or before their launch by agencies if not already in use and make recommendations regarding agency use to ensure that the technology is used in a manner that benefits society and does not have disparate negative impacts on historically and currently marginalized communities or violate their civil rights."[181]

Washington does not define AI, have a working privacy framework, or extend the protections they are recommending outside of the government.[182] Regardless, as a first step, Washington provides an example of how to establish strong intent through law to express that AI should be used for societal good, that it should not disproportionately harm minorities, and that the impacts of AI should be analyzed before implementation.[183]

While these state-wide efforts to push privacy legislation forward are important and necessary, they will always come up short of the comprehensive data and privacy reforms needed to address societal issues because the internet and the data sent by AI entities is not contained within state boundaries.[184]

C. International Comparisons

To create an optimal framework to govern Sexbots, this section examines international laws and frameworks governing data privacy and AI in Singapore, the United States, and the European Union.

1. Singapore

Singapore has a strong model for how legislation can lead AI development and protect the public interest. Their primary piece of legislation governing data privacy is the Personal Data Protection Act (PDPA).[185] Additionally, the PDPA allowed for the creation of the Personal Data Protection Commission (PDPC) to enforce the protections laid out in in the PDPA.[186] The PDPA applies to any organization managing, collecting, using, or disclosing personal data in Singapore.[187] The PDPA sets out baseline standards for data privacy across the

181. *Id.* (emphasis added).

182. *See* Lively, *supra* note 155 (providing a full account of all U.S. states privacy laws at various legislative stages).

183. WASH. REV. CODE. § 43.06D.900 (2020).

184. Adam Strange, *The Argument for a National US Data Privacy Framework*, OPEN ACCESS GOV'T (Sept. 29, 2021), https://www.openaccessgovernment.org/us-data-privacy-framework/121292 [perma.cc/P8LB-UYTR].

185. LIM CHONG KIN, HURTON ANDREWS KURTH LLP, DATA PROTECTION AND PRIVACY 2022 242–256 (Aaron P. Simpson & Lisa J. Sotto eds., 2022).

186. *Id.*

187. *Id.*

private sector.[188] The PDPC is located within the power of Singapore's Ministry of Communications and Information (MCI).[189] Thus, Singapore's data privacy protection frameworks and enforcement derive from federal power.[190] The MCI would be analogous to a bureau within the United States Federal Communications Commission. The PDPC is empowered to demand the stoppage of data collection, destruction of data, force data corrections, allow for access to data collected, and impose penalties to entities found in violation of the PDPA.[191] Under the PDPA, "personal data" is "data about an individual who can be identified from that data, or from that data and other information to which the organization has or is likely to have access."[192] The PDPA also contains provisions requiring organizations to disclose their decision-making policies and practices available upon request.[193]

Singapore's robust privacy framework also includes guidance on the use of AI. On January 21, 2020, Singapore released the second edition of its Model AI Governance Framework.[194] The framework puts forward guiding principles that place the well-being and safety of humans at the forefront to make AI decisions more transparent and explainable.[195] While the AI framework itself is voluntary, the PDPA governs AI-assisted processes,[196] so it is within an organization's best interest to adhere to the framework. The framework is also technology, algorithm, sector, and scale agnostic.[197] This means that the framework sets out broad standards to be followed by all, regardless of what the AI is used for, specific algorithms of the AI, what sector the AI is used in, or the size of the entity using the AI.[198] The main areas the framework advises are the following:

> 1) internal governance structures and measures (how to organize entities to best incorporate values and risks of algorithmic decisions);[199] 2) determining the level of human involvement in AI-augmented decision-making (how much oversight humans should have over an AI process);[200] 3) operations management (best practices for the technical construction of AI processes);[201] and 4) stakeholder

188. *Id*.

189. *Singapore Government Directory*, GOV'T OF SING., https://www.sgdi.gov.sg/search-results?term=pdpc [perma.cc/Y8C8-VHT2] (last visited Oct. 6, 2022) (showing that PDPC employees fall within MCI jurisdiction).

190. *Id*.

191. KIN, *supra* note 186.

192. *PDPA Overview*, PERS. DATA PROT. COMM'N SING., https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act [perma.cc/NB9H-SFK5] (last visited Sept. 26, 2022).

193. Personal Data Protection Act 2012 (2020) § 12 (Sing).

194. PERS. DATA PROT. COMM'N SING., MODEL ARTIFICIAL INTELLIGENCE GOVERNANCE FRAMEWORK 6 (2d ed. 2020) [hereinafter Singapore Model AI Framework].

195. *Id.* at 15.

196. *Id.* at 13.

197. *Id.* at 10.

198. *Id*.

199. *Id.* at 20.

200. *Id.* at 28.

201. *Id.* at 35.

interaction and communication (best practices for building trust with stakeholders when deploying AI processes).[202]

In summary, through the PDPA and the Model AI Governance Framework, Singapore has combined overall data privacy protections that extend into the implementation of AI.

However, there is a difference between stronger data protections and a right to privacy.[203] There is a paradox: the more data protection laws that exist, the more data needs to be kept to ensure compliance with the protections.[204] Although Singapore's data privacy laws and frameworks for dealing with AI far exceeds the United States,[205] the notion that data gleaned from Sexbots should be protected presupposes that the data should be kept at all.[206]

2. United States

The United States has no federal comprehensive privacy framework.[207] Various federal agencies police data and privacy by sector.[208] For example, the Consumer Financial Protection Bureau (CFPB) governs consumer finances through the Grimm-Leach-Bliley Act (GLB).[209] The Department of Health and Human Services governs patient health data through the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[210]

To give an example of how complicated the issue of data privacy can be in healthcare, while most privacy is governed by HIPAA, student immunization records are governed by Family Educational Rights and Privacy Act (FERPA); which also potentially overlaps and conflicts with data governed by the Children's Online Privacy Protection Act (COPPA) which governs some children's data but only up to age thirteen.[211]

The Federal Trade Commission (FTC) has very wide latitude to govern commerce generally through Section 5 of the Federal Trade Commission Act (FTC Act).[212] It states the FTC has the power to regulate "[u]nfair methods of

202. *Id.* at 53.

203. Magdalene Lam, *The "Limited" Assistance of Foreign Jurisprudence: Lessons from India and the United States on Sexuality and Governance*, 42 COLUM. J. GENDER L. 1, 37 ("While it may be possible to derive a theoretical right to privacy from these sources, a realist might argue that the right to privacy remains illusory at best, given the mass surveillance adopted by the Singaporean government.").

204. *Id.* at 36–37 ("'[R]ight to privacy is generally understood as *limiting* government powers that might otherwise interfere with reasonable respect for a private life,' compared to data protection which 'requires an *expansion* of government powers to monitor compliance of both government and third parties that collect, use or disseminate personal data.'").

205. *See infra* Part III.C.2.

206. *See* Lam *supra* note 204, at 36–37 (implying that data protection requires an expansion of power to monitor compliance of personal data).

207. Alex Pearce, *Time for A National Privacy Law? Fragmented Patchwork of State Laws Creates Compliance Issues*, DEL. L., Spring 2020, at 6 ("The CCPA's extraterritorial impact notwithstanding, the United States lacks a comprehensive national privacy law.").

208. Aaron P. Simpson & Lisa J. Sotto, *United States*, *in* 9 DATA PROTECTION AND PRIVACY 2021 296, 296 (Aaron P. Simpson & Lisa J. Sotto eds., 2020).

209. *Id.*

210. *Id.*

211. Strange, *supra* note 185.

212. 15 U.S.C. § 45 (2006).

competition in or affecting commerce" and also declares "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[213] It is through this legislation that the U.S. government can hold actors accountable. The FTC's current litigation against Facebook was through the FTC Act.[214] While that power is useful, "unfair or deceptive acts" without further guidance is comically vague.

It is widely reported that the current quilt-work-like framework for data privacy requires overhauling.[215] Even with states like California leading the way for data privacy frameworks, confusion exists regarding what rules apply to what parties in which specific industries.[216] By federal standards, there is not even agreement on what constitutes personal information in the event of a data breach.[217] Unlike California's CCPA, there is no federal standard for "controller" or "processor" of data.[218]

There is pressure among Congress to update federal privacy laws.[219] However, bipartisan talks are hung up on whether federal regulations should override current state regulations and on what power individual consumers should have under a federal framework.[220] The longer the federal government goes without acting, the more uncertainty will increase as to whether individual state action should govern privacy issues.[221]

U.S. federal law has many references to artificial intelligence. Examples include laws governing the advancement of AI through the National Institute of Science and Technology,[222] the integration of AI into the National Oceanic and Atmospheric Administration,[223] and the ability of the National Science Foundation to fund AI research.[224] However, one of the only definitions of AI comes from the National Artificial Intelligence Advisory Committee:

> The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual

213. *Id.*

214. *The FTC's Facebook Suit: Questions and Answers*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/facebook-q-a [perma.cc/V775-TYQE] (last visited Oct. 6, 2022).

215. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, COVINGTON & BURLING LLP (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law [perma.cc/E6YD-ZMHC].

216. Karen Schuler, *Federal Data Privacy Regulation is on the Way—That's a Good Thing*, INT'L ASS'N PRIV. PROS. (Jan. 22, 2021), https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing [perma.cc/HWW5-XFJV] (explaining the pitfalls of United States data privacy laws and lack thereof).

217. Simpson & Sotto, *supra* note 209.

218. *Id.*

219. Ben Kochman, *Democratic Control Could Break Gridlock on US Privacy Bill*, LAW360 (Jan. 13, 2021, 4:06 PM), https://www.law360.com/articles/1343683/democratic-control-could-break-gridlock-on-us-privacy-bill [perma.cc/7TWF-BTMU] (discussing the political calculations regarding the passage of federal data privacy laws).

220. *Id.*

221. *See id.* ("It may be more realistic to expect momentum to start building in late 2021 or 2022 for federal privacy legislation, which could come on the books around the time California's Privacy Rights Act, which builds on the existing CCPA, is set to go into effect in 2023.").

222. 15 U.S.C. § 278 (h)(1) (2017).

223. 15 U.S.C. § 9442 (2021).

224. 15 U.S.C. § 9451 (2021).

> environments. Artificial intelligence systems use machine and human-based inputs to- (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.[225]

While this definition is not the exclusive definition of AI in the United States,[226] it does express components that states can follow in implementing AI.

3. European Union General Data Protection Regulation (GDPR)

In 2018, the European Union (EU) implemented their data privacy framework, the General Data Protection Regulation (GDPR).[227] The GDPR effectively defines terms governing data transactions. For example, it defines personal data as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[228]

Not only does the GDPR account for the personal identification via data, it also accounts for the use of data to create statistical quantification of a user's personality:

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;[229]

The GDPR also defines points along the chain of data transmission such as, processor, controller, third party, and personal data breach.[230]

To fulfill the goals of the GDPR, each EU member state is required to have an authority dedicated to monitoring GDPR compliance.[231] The GDPR also establishes a European Data Protection Board (EDPB) dedicated to advancing best practices and ultimately resolving member disputes if necessary.[232] Consumer protections are also addressed in the GDPR. There is clear authority

225. 15 U.S.C. § 9401 (2021).

226. *See* LAURIE A. HARRIS, CONG. RSCH. SERV., R46795, ARTIFICIAL INTELLIGENCE: BACKGROUND, SELECTED ISSUES, AND POLICY CONSIDERATIONS 1 (2021) (explaining there is no single, commonly agreed upon definition of AI).

227. *What is GDPR, the EU's New Data Protection Law?,* PROTON TECHS. AG, https://gdpr.eu/what-is-gdpr [perma.cc/V7G3-DXPU] (last visited Oct. 6, 2022).

228. Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1 (EU).

229. *Id.*

230. *Id.*

231. *Id.* at art. 51.

232. *Id.* at art. 68, 70.

for remedies against controllers or processors who mishandle data.[233] These penalties and fines can be levied by each member state's supervisory authority or the EDPB itself.[234]

Although the GDPR has no reference to the term "artificial intelligence," the EU does have their own proposed Artificial Intelligence Act (AI Act).[235] The AI Act defines AI as "software that is developed with one or more of the techniques and approaches listed in Annex I[236] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with . . . ."[237]

As the AI Act is a proposal, it is still a work in progress. The given definition for AI has been critiqued as being overly broad.[238] Defining AI by techniques and approaches like statistical analysis, logic induction, and machine learning could apply to all algorithms.[239] At the very least, the European Council has called for the development of this technology to meet "ethical standards" and to identify uses of AI that could be considered "high-risk."[240]

IV. RECOMMENDATION

A. Why Illinois Should Lead on Sexbot Regulation

Illinois should take proactive steps to regulate privacy issues that will be exacerbated by Sexbot technology. In the first six months of 2019, billions of pieces of personal data were hacked, leaked, or stolen.[241] The ease with which intimate data regarding people's most private behavior could be accessed by unknown third parties is untenable.[242] Even if data is not hacked and is held by the company that manufactures the Sexbot, the current state and national frameworks for data privacy are unclear.[243] For example, even if a company effectively protects intimate data from a breach, there is nothing mandating them

233. *Id.* at art. 82.

234. *Id.* at art. 83–84.

235. *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at 1, COM (2021) 206 final *(*Apr. 21, 2021) [hereinafter *EU AI Act Proposal*].

236. *Id.* at 39; *see also Annexes to the Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at 1, COM (2021) 206 final *(*Apr. 21, 2021) (specifying such techniques and approaches include machine learning, deductive engines, and statistical optimization, amongst others).

237. *EU AI Act Proposal*, *supra* note 236, at 39.

238. NATHALIE SMUHA ET AL., LEADS LAB @ UNIV. OF BIRMINGHAM, HOW THE EU CAN ACHIEVE LEGALLY TRUSTWORTHY AI: A RESPONSE TO THE EUROPEAN COMMISSION'S PROPOSAL FOR AN ARTIFICIAL INTELLIGENCE ACT 14 (2021).

239. *Id*.

240. *EU AI Act Proposal*, *supra* note 236, at 2.

241. Winder, *supra* note 111.

242. *See* Jones, *supra* note 72 (examining the Canadian smart-dildo hack leaking intimate user data).

243. *See* PRIV. INT'L, *supra* note 67 (discussing the Arkansas Bates case and International Privacy's subsequent investigation into Amazon's response to their questions regarding Echo's data gathering capabilities); Kelly & Statt, *supra* note 122 (similar).

from using that data for their own alternative purposes.[244] If the Illinois legislature knowingly does nothing, they will be complicit in enabling harmful practices to consumers.

Creating a workable framework to govern Sexbots would be pivotal to become a national leader on a pressing issue that will only grow in prevalence.[245] Ten percent of young people are already open to intimate relationships with robots, and technology only advances.[246] An analogous issue is that of vehicle emissions standards. California took more stringent measures than all other states and the federal government.[247] By ambitiously attacking climate-change emissions goals, other states were emboldened to join on to California's standards.[248] As a result, manufacturers adhered to their standard under fear of not being able to access their market, and this led to an increased shift towards electric and low-emission vehicles.[249] Illinois should follow this model of protecting citizen's intimate data recorded by Sexbots and push the vanguard of data protection and AI governance forward.

B. What Illinois's Sexbot Legislation Should Include

First, Illinois should take proactive measures to pass a data privacy framework that governs the use of consumer data generally. Illinois should expand its Personal Information Protection Act (PIPA) towards adopting California's definition of personal information to include internet data, geographic data, and audio or visual information stored by electronic devices.[250] Additionally, Illinois should add to their definitions of who possesses data in PIPA. Currently, PIPA's language on data collectors could be construed very broadly, but it lacks references to other parties on the chain of the transmission of data like processor, handler, or third party.[251] Based on GDPR, Illinois should add definitions of data processors and third parties to PIPA to further protect data as it is shared from collectors to other parties who may handle it.[252]

Illinois should also expand its own definition of personal information. As constituted under PIPA, "personal information" is mostly defined as information

244. *See* PRIV. INT'L, *supra* note 67 (discussing questions surrounding how Amazon and Google handle personal information collected from smart devices).

245. Suk Gersen, *supra* note 141, at 1795 ("Robots that are currently commercially available are relatively unsophisticated, but rapid advances in the field make it likely they will eventually approach the realistic behavior of the robot characters of *Westworld*, *Humans*, and *Ex Machina*.").

246. Mascarenhas, *supra* note 11; *see also* Fisher, *supra* note 12 (discussing the trend of young people taking part in on-demand chatbot relationships).

247. *See* Nicholas Bryner & Meredith Hankins, *Why California Gets to Write its Own Auto Emissions Standards: 5 Questions Answered*, CONVERSATION (Apr. 6, 2018, 6:46 AM), https://theconversation.com/why-california-gets-to-write-its-own-auto-emissions-standards-5-questions-answered-94379 [perma.cc/54FF-FZG6] (outlining a history of heightened California automobile emission standards).

248. Rachel Frazin, *More States Follow California's Lead on Vehicle Emissions Standards*, THE HILL (Feb. 28, 2021, 8:00 AM), https://thehill.com/homenews/state-watch/540795-more-states-follow-californias-lead-on-vehicle-emissions-standards [perma.cc/CAX7-EXEA] (discussing states' shift towards California's emissions standards).

249. *Id.*

250. *Supra* Part III.B.2.

251. 815 ILL. COMP. STAT. 530/5 (2017).

252. *See* Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) (EU) (defining terms within the GDPR).

relating to accounts and records like insurance, driver's licenses, and bank accounts.[253] Illinois should add the language from PHPA governing electronic communications to the definition of personal information to include any "signs, signals, data, writings, images, video, audio, or intelligence of any nature" that could identify an individual.[254]

By strengthening the definitions of who possess data and what constitutes personal data, Illinois would position itself better for the proliferation of Sexbots without explicitly legislating on Sexbots while strengthening privacy laws overall.

Regarding AI, Illinois should create a model AI framework based on Singapore's model. A framework that governs how to organize entities to handle AI, how much oversight should go into AI, how to technically construct AI algorithms responsibly, and communication strategies around AI deployment are current best practices.[255] Like in Singapore, an AI framework supported by robust privacy legislation gives the framework further regulatory strength.[256] These advancements in AI oversight would also strength entities' protective storage of biometric information as mandated by BIPA.[257]

Illinois should incorporate a mission statement like that of Washington state to mandate that AI be "used in a manner that benefits society and does not have disparate negative impacts on historically and currently marginalized communities or violate their civil rights."[258]

Illinois can ban a practice or good that is not in the best interest of its citizens.[259] Sexbots could potentially raise enough moral or legal issues that it is better off banning them. Organizations like CASR are already calling for governments to take a firm stance that society should abolish the development of Sexbots in the form of women and girls.[260] Their perspective is grounded in the belief that replacing women with machines is inherently dehumanizing and Sexbots' existence leads to a reinforcement of sexual power structures where one party, typically women, is not seen as human.[261] However, if Illinois bans anything that is permitted federally and bordering states do not follow suit, residents will simply find the goods across borders.[262] Without a federal ban on

253. 815 ILL. COMP. STAT. 530/5 (2017).
254. 5 ILL. COMP. STAT. 855/5 (2022).
255. *Supra* Part III.C.1.
256. *Id*.
257. 720 ILL. COMP. STAT. 14/15 (2008).
258. WASH. REV. CODE. § 43.06D.900 (2020).
259. *See Illinois Becomes the First State to Ban Police from Lying to Juveniles During Interrogations*, INNOCENCE PROJECT (July 15, 2021), https://innocenceproject.org/illinois-first-state-to-ban-police-lying [perma.cc/X4CY-LVNL] (discussing Illinois's ban on the practice of using deception in the detention of minors).
260. CAMPAIGN AGAINST SEX ROBOTS, https://campaignagainstsexrobots.org [perma.cc/S9X3-ZK4A] (last visited Sept. 26, 2022) (listing its goals on its home webpage).
261. *See* Kathleen Richardson, *The Asymmetrical 'Relationship': Parallels Between Prostitution and the Development of Sex Robots*, 45 ACM SIGCAS COMPUTS. & SOC'Y 290, 292 (2015) (discussing how the development of sex robots will further reinforce relations of power that do not recognize both parties as human).
262. *See* Philip J. Cook et al., *Some Sources of Crime Guns in Chicago: Dirty Dealers, Straw Purchasers, and Traffickers*, 104 J. CRIM. L. & CRIMINOLOGY 717, 725 (2014) (claiming that many firearms used by gangs in Cook County come from Indiana).

Sexbots, Illinois would be better served strengthening their data privacy and AI frameworks to minimize the negative impacts Sexbots may cause.

There is the case to be made that states should not be undertaking such robust privacy regulations, and a centralized framework should result from the federal government that governs the entire United States.[263] In theory, that would be fine. In practice, it would possibly end up like the current patchwork framework where three different laws would overlap and confuse what governs children's healthcare information privacy.[264] Also, partisan gridlock on this issue threatens potential legislation on such a framework getting passed.[265] The issue of sensitive consumer information being shared with AI technology and other entities without owner's consent cannot wait for the federal government to legislate effectively.[266]

Thus, by focusing on expanding the on the definition of personal information, widening the regulation on those who handle personal data, and creating a model AI framework to recommend best practices and implementation across society, Illinois can create effective policy that will govern Sexbots and all future AI technologies.

V. CONCLUSION

Sexbots will continue as a widespread societal reality.[267] The current state of privacy laws in Illinois and the United States are not ready for this technological advance.[268] The United States laws on artificial intelligence lag significantly behind other developed nations.[269] Illinois's laws governing personal information do not include many forms of data transmitted by smartphones and computers.[270] As currently constituted, ownership of sensitive data from household devices from Sexbots will evolve.[271] The current overall regulatory situation is fairly bleak considering the impact of Sexbot technology has the potential to fundamentally alter the way humans behave.[272]

That does not mean the situation is hopeless. Illinois can strengthen its own definition of personal information, widen the reach of their laws to compel all parties in possession of data to protect it, and create a modernized AI framework

263. *See* Strange, *supra* note 185 (arguing that federal legislation is needed because the internet is not contained within one state's borders).

264. *Id.*

265. Kochman, *supra* note 220 (discussing the political calculations regarding the passage of federal data privacy laws).

266. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [perma.cc/42HJ-ALNP] (discussing how existing legislation has failed to slow an increase in data breaches).

267. Crocker, *supra* note 1 (describing how robots with artificial intelligence capacities are currently on the market).

268. Shen, *supra* note 25 (highlighting the issues with child safety, data privacy, and legal frameworks governing Sexbots).

269. *Supra* Part III.C.1, Part III.C.3.

270. 815 ILL. COMP. STAT. 530/5 (2017).

271. *See* Bohn, *supra* note 70 (discussing how Apple knows many things about its users and how Apple has the capacity to turn information of its users to the government if legally required to do so); Ng, *supra* note 66 (discussing collection of personal information by Amazon).

272. Christakis, *supra* note 14.

to ensure future generation technology is used for societally productive purposes.

The future of Sexbots is on the horizon, but the regulatory issues they will create are here today. Illinois has the opportunity to lead on data privacy, AI, and consumer protection. The key is to enact the changes to ensure a more secure future before we stare it straight in its humanoid face.