

IF YOU SEE SOMETHING, SAY SOMETHING:
CAN ARTIFICIAL INTELLIGENCE HAVE A DUTY TO REPORT
DANGEROUS BEHAVIOR IN THE HOME?

JASON ZENOR[†]

ABSTRACT

Artificial intelligence (AI) digital assistants, such as Amazon’s Echo Alexa and Apple’s Siri, are becoming quite common in our homes. Today, these voices typically come from a small speaker. But soon, they will be replaced by devices that appear more human than robot. As a result, our relationships with them will change. We will talk to them and share information, including our secrets, with them. Of course, we will have to trust them with this information. But should we? If an AI is in the home and monitoring a person, what should it do if someone is exhibiting signs of alcoholism, depression, or violence? Accordingly, this Article postulates how changes in our personal relationship with AI could lead to changes in how privacy protections are viewed. First, this Article examines nascent issues of AI assistants publicizing private activities and how these issues could evolve in the future. Next, this Article outlines privacy law as it pertains to activity in the home. Finally, this Article postulates how cultural expectations of privacy could erode in the future and offers suggestions on how to model laws that balance privacy with public safety.

TABLE OF CONTENTS

INTRODUCTION	840
I. FROM PERSONAL DIGITAL ASSISTANTS TO DOMESTIC SMART ROBOTS.....	842
<i>A. Development of Voice Assistants</i>	842
<i>B. Future of In-Home AI</i>	843
II. PRIVATE VIOLENCE.....	846
<i>A. Suicide</i>	846
<i>B. Domestic Abuse</i>	848
<i>C. Current Use of AI in Prediction and Prevention</i>	848
1. Voice Assistants	848
2. Apps and Chatbots	850
III. LEGAL PROTECTION OF INFORMATION	851
<i>A. Expectation of Privacy</i>	851
1. Search and Seizure	852

[†] Jason Zenor, Associate Professor, School of Communication Media & the Arts, SUNY-Oswego.

2. Intrusion upon Seclusion.....	853
3. Publication of Private Facts	854
B. Confidential Relationships	854
1. Privileged Communication.....	854
2. Duty to Report.....	855
3. Failure to Report and Negligence	856
IV. ANALYSIS.....	857
A. In-Home AI: Houseguest or Roommate?	857
B. Duty to Report: Possible Legal and Ethical Duties?	858
C. Butterfly Effect: Issues with a Duty to Report for In-Home AI...	861
1. Initiating the Justice System.....	861
2. False Negatives and False Positives.....	862
3. Protecting Sensitive Information.....	864
CONCLUSION.....	865

INTRODUCTION

In 2017, a domestic disturbance reported in Albuquerque, New Mexico, became national news.¹ The disturbance started when Eduardo Barros accused his girlfriend of cheating on him because she received text messages on her phone.² Eventually, the situation escalated and Barros wielded a gun and threatened his girlfriend with it.³ During the altercation, Barros asked his girlfriend if she had called the police—but she had not.⁴ Moments later, 911 dispatchers called the home.⁵ Upon seeing the number on caller ID, Barros became violent, physically assaulted his girlfriend, and held her hostage once the police arrived.⁶ After a long standoff, Barros was taken into custody.⁷ His victim was injured, but fortunately, she survived.⁸

After the incident, there was still an unanswered question: Who called the police? Investigators were surprised when they realized that Amazon Echo’s Alexa had called.⁹ The call likely happened when Barros asked his girlfriend if she had called the police, prompting Alexa to call 911.¹⁰

1. Mikael Thalen, *Man Arrested for Alleged Domestic Violence after Alexa Calls the Cops*, DAILY DOT (July 12, 2019, 1:06 PM), <https://www.dailydot.com/debug/man-arrested-domestic-violence-alexa/>.

2. Joshua Rhett Miller, *Alexa Calls Cops on Man Allegedly Beating His Girlfriend*, N.Y. POST (July 10, 2017, 11:27 AM), <https://nypost.com/2017/07/10/alexa-calls-cops-on-man-allegedly-beating-his-girlfriend/>.

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

10. *Id.* It is unclear what really happened. Police recordings reveal that the victim had said, “Alexa, call 911.” But Amazon disputes that Alexa was able to make the 911 call. See Christopher Melee, *Did an Echo Call 911 During a Domestic Assault? Amazon Says No.*, N.Y. TIMES (July 11, 2017), <https://www.nytimes.com/2017/07/11/business/amazon-echo-911-emergency.html>.

Of course, Alexa did not decide to call the police on its own. Alexa could place the call because the victim had 911 in her phone contacts or directly connected the Alexa to a landline.¹¹ But Alexa did require activation first (e.g., “Hey Alexa, call 911”).¹² Phone voice assistants allow people to call 911 without physically dialing the number, and in-home digital assistants (e.g., Amazon’s Echo) are adopting this technology.¹³ But what if the in-home artificial intelligence (AI) did not have to wait for user activation? What if it sensed danger and recognized a duty to call the authorities on its own?

The purchase of home smart speakers now outpaces that of smartphones.¹⁴ With the adoption of such technology comes privacy concerns—specifically, outside parties accessing sensitive information.¹⁵ There are concerns about police conducting searches, hackers stealing information, and companies collecting sensitive data.¹⁶ Of course, these issues are about outside parties breaking into personal privacy bubbles to access sensitive information people want to protect. But what about sensitive information that people may want hidden, but others should know about?

This Article focuses on private behavior that can be dangerous for the individual and others. For example, consider a person who is at home excessively drinking, taking dangerous drugs, showing signs of deep depression, or is at risk of becoming violent. Individuals might hide these behaviors in public or from those close to them. Yet, personal contact and outreach is often the only hope for preventing individuals from hurting themselves or others. So, could in-home AI be the solution? Could it recognize risks for violent behavior? Should in-home AI even be able to offer help? If violence is imminent, should the AI system be compelled to report it?

Accordingly, this Article examines the legal and ethical implications of in-home AI encountering sensitive, private issues, such as depression, addiction, abuse, and violence. First, this Article examines the use of AI

11. Melee, *supra* note 10.

12. *Id.*

13. *Id.* There are many terms used to describe the technology and many are used interchangeably. For the purpose of this Article, this Article uses “voice assistant” for AI that speaks such as Amazon’s Alexa, Apple’s Siri and Google’s Assistant. These voice assistants are available in many devices such as phones and smart speakers like the Amazon Echo. It refers to in-home AI because the voice assistant will be in a domestic setting, like a smart speaker or smart home. In the future, this term could also include more social robots. See generally Valarie K. Blake, *Regulating Care Robots*, 92 TEMP. L. REV. 551, 572–73 (2020).

14. Brad Moon, *Smart Speaker Sales are Growing Faster than Smartphones in the U.S.*, INVESTORPLACE (Jan. 16, 2018, 10:13 AM), <https://investorplace.com/2018/01/smart-speaker-sales-faster-smartphones-u-s/>.

15. See, e.g., Graham Johnson, *Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards*, 11 WASH. U. JURIS. REV. 345, 352–60 (2019); Allegra Bianchini, *Always on, Always Listening: Navigating Fourth Amendment Rights in a Smart Home*, 86 GEO. WASH. L. REV. ARGUENDO 1, 4–5 (2018); Steven I. Friedland, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy*, 119 W. VA. L. REV. 891, 892 (2017).

16. See Johnson, *supra* note 15; Bianchini, *supra* note 15; Friedland, *supra* note 15.

in homes.¹⁷ This Article then outlines how AI is used in predicting and preventing private violence.¹⁸ Next, this Article examines the laws of privacy, confidentiality, and mandatory reporting.¹⁹ Finally, this Article analyzes the role of in-home AI, how it could be used to report risks and acts of violence, and the ethical issues it creates.²⁰

I. FROM PERSONAL DIGITAL ASSISTANTS TO DOMESTIC SMART ROBOTS

A. Development of Voice Assistants

Voice assistants have existed for decades.²¹ In the 1960s, IBM created a tool called Shoebox, which could recognize sixteen spoken words and the numbers zero through nine.²² In the 1970s, a Carnegie Mellon University and U.S. military collaboration produced Harpy, a program that could recognize over one thousand words—the same as the vocabulary of a three-year-old child.²³ By the end of the 1980s, many devices had applications that could respond to the human voice, including dolls such as Julie, created by Worlds of Wonder.²⁴ In the early 1990s, Apple included a speech recognition program called Macintalk into its Mac computers,²⁵ and IBM introduced Simon, a personal digital assistant that included a voice assistant.²⁶

Today, many of the devices people use daily have a built-in voice assistant, including phones, televisions, and cars.²⁷ The most recognizable voice assistants are Apple's Siri (introduced in 2011), Google's Assistant (introduced in 2016), Microsoft's Cortana (introduced in 2014), and

17. See *infra* Part I.

18. See *infra* Part II.

19. See *infra* Part III.

20. See *infra* Part IV.

21. IBM, *Archives: IBM Shoebox*, https://www.ibm.com/ibm/history/exhibits/specialprod1/specialprod1_7.html.

22. *Id.*

23. Katia Moskvitch, *The Machines that Learned to Listen*, BBC (Feb. 15, 2017), <https://www.bbc.com/future/article/20170214-the-machines-that-learned-to-listen> (outlining a history of mechanized voice assistants).

24. See Gene Franz, James Reimer, & Richard Wotiz, *Julie: The Application of DSP to a Consumer Product*, SPEECH TECH., 83–84 (1988). Thomas Edison created the first talking doll in 1890 that included recordings of adults impersonating children. Neda Ulaby, *Edison's Talking Doll Can Now Provide the Soundtrack to Your Nightmares*, NPR: THE TWO-WAY (May 5, 2015, 5:02 PM), <https://www.npr.org/sections/two-way/2015/05/05/404445211/edisons-talking-dolls-can-now-provide-the-soundtrack-to-your-nightmares#:~:text=Now%2C%20new%20technology%20has%20made%20hearing%20them%20possible%20for%20the,worker%20imitating%20a%20little%20girl>.

25. See, e.g., Stephen Shankland, *How Apple Uses AI to Make Siri Sound More Human*, CNET (Aug. 23, 2017, 3:17 PM), <https://www.cnet.com/news/apple-ai-machine-learning-makes-siri-sound-human-on-ios-11/>.

26. Doug Aamoth, *First Smartphone Turns 20: Fun Facts About Simon*, TIME (Aug. 18, 2014, 4:23 PM), <https://time.com/3137005/first-smartphone-ibm-simon/>.

27. See, e.g., Bret Kinsella, *New Report: Over 1 Billion Devices Provide Voice Assistance Today and Highest Usage is in Smartphones*, VOICEBOT.AI 1, 3 (Nov. 13, 2018), <https://voicebot.ai/2018/11/13/new-report-over-1-billion-devices-provide-voice-assistant-access-today-and-highest-usage-is-on-smartphones/>; Daniel Wroclawski, *Which Appliances Work With Amazon Alexa, Google Home, and More*, CONSUMER REPS. (Mar. 2, 2018), <https://www.consumerreports.org/appliances/smart-appliances-that-work-with-amazon-alexa-google-home-and-more/>.

Amazon's Alexa (introduced in 2014).²⁸ These voice assistants are often in home devices such as smart speakers like Amazon's Echo, Apple's HomePod, and Google's Nest.²⁹

Voice assistants rely on “wake words”—usually the voice assistant's name—for activation (e.g., “Hey Alexa, . . .”).³⁰ Wake words are built into the program and cannot be customized (though users may have a choice of several words).³¹ Once a person says the wake words, the device can “communicate” with the user.³² Designers make wake words simple and distinct so nothing is lost in translation of everyday human speech patterns (e.g., using “Lex” as a nickname for Alexa).³³ The voice assistant does not technically understand the user's speech; instead, it responds to exact words and fulfills the tasks requested.³⁴ But, once activated, the AI system can have a rather convincing conversation with the user (though it will still apologize often for not understanding).³⁵

B. Future of In-Home AI

Because voice assistants anticipate activation, they continuously listen while the device is on. As a result, people may not realize when the device is listening.³⁶ Moreover, some smart devices are built to go beyond

28. Diana Ramos, *Voice Assistants: How Artificial Intelligence Assistants Are Changing Our Lives Every Day*, SMARTSHEET (Apr. 16, 2018), <https://www.smartsheet.com/voice-assistants-artificial-intelligence>. Most of these voice assistants are female voices by default and people refer to the voice as a she, as if a person, and not it, as if a robot. See Chandra Steele, *The Real Reason Voice Assistants are Female (and Why it Matters)*, PC MAG (Jan. 4, 2018), <https://www.pcmag.com/opinions/the-real-reason-voice-assistants-are-female-and-why-it-matters>.

29. *Smart Audio Report*, NAT'L PUB. MEDIA (April 2020), <https://www.nationalpublicmedia.com/insights/reports/smart-audio-report/>. They are also used extensively in many industries including education, health, and security. Forbes Technology Council, *Council Post: 13 Industries Soon to be Revolutionized by AI*, FORBES (Jan. 16, 2019, 7:00 AM), <https://www.forbes.com/sites/forbestechcouncil/2019/01/16/13-industries-soon-to-be-revolutionized-by-artificial-intelligence/?sh=d535bb63dc18>.

30. See, e.g., Rowan Trollope, *7 Things You Didn't Know about Wake Words*, MEDIUM (Nov. 29, 2017), <https://medium.com/@rowantrollope/7-things-you-didnt-know-about-wake-words-d4e9e041d11d>.

31. *Id.*; see also Stephen Harrison, *Don't Call It "Siri": Why the Wake Word Should Be "Computer"*, SALON (Nov. 26, 2017, 4:00 PM), <https://www.salon.com/2017/11/26/dont-call-it-siri-why-the-wake-word-should-be-computer/>.

32. Current voice assistants can only “understand” a few words. As the *New York Times* described them: “Think of Echo like a dog: It's always listening, but it understands only ‘cookie,’ ‘walk,’ or ‘Buddy.’ Everything else goes right over its head.” Grant Clauser, *Amazon's Alexa Never Stops Listening to You*, N.Y. TIMES: WIRECUTTER (Aug. 8, 2019), <https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/>.

33. See, e.g., Trollope, *supra* note 30.

34. Clauser, *supra* note 32.

35. See Yolande Strengers, *Amazon Echo's Alexa is Programmed to Always Apologize—Especially When It's not Her Fault*, NBC NEWS (Mar. 2, 2021, 2:30 AM), <https://www.nbcnews.com/think/opinion/amazon-echo-s-alexa-programmed-always-apologize-especially-when-it-nena1259001>. Some have criticized the subservient nature of the voice assistants since most are female voices by default. See, e.g., Ian Bogost, *Sorry, Alexa is Not a Feminist*, ATLANTIC (Jan. 24, 2018), <https://www.theatlantic.com/technology/archive/2018/01/sorry-alexa-is-not-a-feminist/551291/>.

36. Examples of some technology that is “always on”: Google's Chrome, Xbox Kinect, and Mattel's Hello Barbie. Millie Dent, *The New Generation of 'Genuinely Creepy' Electronic Devices*, FISCAL TIMES (July 16, 2015), <https://www.thefiscaltimes.com/2015/07/16/New-Generation-Genuinely-Creepy-Electronic-Devices>.

responding and observe and analyze their environment to better serve the user.³⁷ For example, a smart vacuum, such as a Roomba, will take in information about a room it vacuums to improve its service.³⁸ Smart homes can automatically control many parts of the homes, such as locks, lights, doors, and appliances.³⁹ They can also alert a homeowner to when family members are home by using phone GPS applications.⁴⁰

Smart appliances usually serve a single function—vacuum, cook, refrigerator, etc. User relationships with them are utilitarian and one-way.⁴¹ But the relationship to voice assistants in smart speakers can be different. People still ask them questions and give them commands, but also use them for more social reasons, including companionship.⁴² Thus, for many, the relationship with in-home AI has already moved beyond utilitarian and is becoming “parasocial,” akin to humans’ relationships with pets.⁴³

This social relationship will only grow as in-home AI moves beyond small speakers and are placed in anthropomorphic robots.⁴⁴ When this happens, AI will be continuously present—speaking, listening, observing, and recording.⁴⁵ With in-home robots, people may never feel alone again while at home. Robots will be able to move around the house and some may roam freely.⁴⁶ Even if stationary, they will have advanced technology that

37. See generally Susan Allen, *Privacy in the Twenty-First Century Smart Home*, 19 J. HIGH TECH. L. 162, 177–80 (2018) (discussing how smart tech in the homes monitor people).

38. Like most commercial tech products, the Roomba evolved from technology used by the military and NASA. Kyle L. Wiggers, *Sweeping Changes: How iRobot Evolved from Military Robots to Autonomous Vacuums*, VENTURE BEAT (June 18, 2019, 6:30 AM), <https://venturebeat.com/2019/06/18/sweeping-changes-how-irobot-evolved-from-military-robots-to-autonomous-vacuums/>.

39. Aliza Vigderman & Gabe Turner, *Your Complete Smart Home Guide*, SECURITY.ORG, <https://www.security.org/smart-home/> (last updated Mar. 23, 2021).

40. See *id.* With the advancement of other technology and robotics, the “intelligence” of homes will grow exponentially over the next several years. See Patrick Lucas Austin, *What Will Smart Homes Look Like 10 Years From Now*, TIME (July 25, 2019, 6:18 AM), <https://time.com/5634791/smart-homes-future/>.

41. Even with simplistic tasks, the nuance and variety of language can make it difficult to program voice activate appliances. See Ellen Byron, *Does Your Washing Machine Understand You? How to Talk to Appliances*, WALL ST. J. (Nov. 19, 2017), <https://www.wsj.com/articles/does-your-washing-machine-understand-you-how-to-talk-to-appliances-1510941331>. General Electric’s product designers summed up the difficulty of giving appliances a voice: “You don’t want it to sound too human, because then you’re talking to an inferior human . . . [t]here’s this level of more than a machine but less than a person, and we’re trying to find that balance.” *Id.*

42. Graeme McLean & Kofi Osei-Frimpong, *Hey Alexa ... Examine the Variables Influencing the Use of Artificial Intelligent in-Home Voice Assistants*, 99 COMPUTS. HUM. BEHAV. 28, 35 (2019). This happens most often in homes where there is only one or two people present. *Id.*

43. Yeibeech Jang, *Exploring User Interaction and Satisfaction with Virtual Personal Assistant Usage through Smart Speakers*, 33 ARCHIVES OF DESIGN RSCH. 127, 129 (2020). Parasocial interaction research has been well developed in audience studies and how people develop seemingly real relationships with celebrities they never meet. See generally PARASOCIAL POLITICS: AUDIENCES, POP CULTURE, AND POLITICS 45–46, 49 (Jason Zenor ed. 2014).

44. Some authors have considered whether this social relationship could evolve into an intimate relationship. See Kate Letheren & Jonathan Roberts, *My Robot Valentine: Could You Fall in Love with a Robot?*, THE CONVERSATION (Feb. 10, 2016, 2:08 PM), <https://theconversation.com/my-robot-valentine-could-you-fall-in-love-with-a-robot-53564>.

45. See generally Austin, *supra* note 40.

46. See, e.g., Ben Ashman, *5 Fascinating Robots that Help Around the House*, TOP BUS. TECH (July 15, 2019), <https://tbtech.co/5-fascinating-robots-that-help-around-the-house/>.

could allow them to hear acutely throughout a home⁴⁷ or see through walls.⁴⁸ Human relationship with anthropomorphic robots could go to either extreme—where people forget it is a robot and reveal too much or forget that it is more than a simple machine and capable of advanced surveillance.⁴⁹

In-home AI will have access to private information that people share intentionally, but also inadvertently.⁵⁰ From this information—combined with troves of big data it can access as a connected device—it could predict human behavior.⁵¹ Algorithms already do this through user searches and can suggest advertisements, products, videos, and search queries.⁵² Recently, Amazon announced that Alexa will be able guess users' next questions.⁵³ If a user asked Alexa, "What time is it in London?" it may follow up with a question of, "Do you want me to call Mom?" (who lives in London). Amazon claims this service is about inferring the customers' "latent goals"⁵⁴ and tries to make the conversation between the AI system and the human user seem more natural.⁵⁵

With the ability of goal prediction, in-home AI can make suggestions for grocery lists, fitness needs, or songs to cheer people up, just by observing human behavior and environment.⁵⁶ Much like a roommate who says, "We need more eggs" or, "We should go for a walk," these interactions could be beneficial and welcomed.⁵⁷ But if in-home AI acts like a family

47. See, e.g., Adam Conner-Simmons & Rachel Gordon, *Artificial Intelligence Senses People Through Walls*, MIT NEWS (June 12, 2018), <https://news.mit.edu/2018/artificial-intelligence-senses-people-through-walls-0612>.

48. Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1133 (2015).

49. Margot E. Kaminski, Matthew Rueben, William D. Smart, & Cindy M. Grimm, *Averting Robot Eyes*, 76 MD. L. REV. 983, 994–96 (2017) (describing concerns about AI protecting privacy, respecting boundaries, and management and understanding of social relationships).

50. See Allen, *supra* note 37.

51. Jeremy Fain, *How Deep Learning Can Help Predict Human Behavior*, FORBES (Apr. 30, 2018, 9:00 AM), <https://www.forbes.com/sites/forbesagencycouncil/2018/04/30/how-deep-learning-can-help-predict-human-behavior/?sh=2e793f875554>.

52. *Id.*

53. Rachel Sanders, *Amazon Says Alexa Can Predict 'Latent' Requests—Even If You Don't Say Them*, FORBES (Nov. 11, 2020, 2:03 PM), <https://www.forbes.com/sites/rachel-sandler/2020/11/11/amazon-says-alexa-can-predict-latent-requests-even-if-you-dont-say-them/?sh=147d8fce45cf>.

54. *Id.*

55. *Id.*

56. See Austin, *supra* note 40. As Professor Calo predicts: "With enough data about you and the population at large, firms, governments, and other institutions with access to AI will one day make guesses about you that you cannot imagine — what you like, whom you love, what you have done." Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 421 (2017).

57. See, e.g., Alessandro Di Nuovo, *Robot Carers Could Help Lonely Seniors — They're Cheering up Humans Already*, THE CONVERSATION (Nov. 23, 2018, 7:05 AM), <https://theconversation.com/robot-carers-could-help-lonely-seniors-theyre-cheering-humans-up-already-106181>.

member or a friend, it may also need to show tough love by telling people the things they do not want to hear.⁵⁸

II. PRIVATE VIOLENCE

A. Suicide

In 2018, 48,344 people died by suicide in the United States—a 35% increase from twenty years ago.⁵⁹ It is the second leading cause of death for people aged ten to thirty-four.⁶⁰ In 2019, an estimated 12 million U.S. adults had suicidal thoughts, and of them, 3.5 million made suicide plans, with about one-third following through on the plan.⁶¹

To predict suicide, certain variables correlate with increased risk.⁶² For example, males are three times more likely to commit suicide than females and are most likely to use a firearm.⁶³ People who identify as American Indian or white are roughly two times more likely to die by suicide than those who identify as Black.⁶⁴ Youth who identify as LGBTQ are three times more likely to attempt suicide than those who do not identify as LGBTQ.⁶⁵ Suicide rates are higher in rural areas than in urban areas.⁶⁶ Additionally, people who perpetrate mass shootings often show signs of suicidal tendencies beforehand.⁶⁷

Though people attempt suicide for many reasons—some unknown—health-care professionals know that the most common drivers are

58. Most critics argued that AI will be curated to be subservient and enabling. *See, e.g.*, Monty Munford, *Artificial Intelligence –Enemy Of The People Or Friend Of The Lazy And Inept?*, FORBES (Oct. 28, 2018, 1:02 PM), <https://www.forbes.com/sites/montymunford/2018/10/28/artificial-intelligence-enemy-of-the-people-or-friend-of-the-lazy-and-inept/?sh=17a6e5d17649>.

59. *Suicide*, NAT'L INST. OF MENTAL HEALTH, <https://www.nimh.nih.gov/health/statistics/suicide.shtml> (last visited Apr. 23, 2021).

60. *Id.* Suicide is the fourth leading cause of death for persons aged 35–54. *Id.*

61. *Id.* Thirty-five percent of the sample did not take the NIMH survey. The organization postulates that people with suicidal thoughts may be less likely to respond to such a survey, thus, actual numbers could be higher. *Id.*

62. *Suicide Statistics*, AM. FOUN. SUICIDE PREVENTION, <https://afsp.org/suicide-statistics/> (last visited Apr. 23, 2021).

63. Firearms account for more than 50% of suicides. *Suicide Statistics*, *supra*, note 62. Suicides account for 60% of all firearms deaths in the United States compared to homicides (37%), police and accidental shootings (3%), and mass shootings (0.2%). Tom Wickizer, Evan V. Goldstein, & Laura Prater, *More Mental Health Care Won't Stop the Gun Epidemic, New Study Suggests*, THE CONVERSATION (Oct. 7, 2019, 5:20 PM), <https://theconversation.com/more-mental-health-care-wont-stop-the-gun-epidemic-new-study-suggests-124253>. Owning a firearm doubles the likelihood that people will contemplate suicide. *Id.* For those with mental illness, the likelihood increases sevenfold. Miranda Lynne Baumann & Brent Teasdale, *Allowing Mentally Ill People to Access Firearms is not Fueling Mass Shootings*, THE CONVERSATION. (Jan. 3, 2018, 11:33 PM), <https://theconversation.com/allowing-mentally-ill-people-to-access-firearms-is-not-fueling-mass-shootings-89336>.

64. *Suicide Statistics*, *supra* note 62.

65. *Suicide Statistics and Facts*, SUICIDE AWARENESS VOICES OF EDUC., <https://save.org/about-suicide/suicide-facts/> (last visited Apr. 23, 2021).

66. KRISTEN PETTRONE & SALLY C. CURTIN, URBAN-RURAL DIFFERENCES IN SUICIDE RATES, BY SEX AND THREE LEADING METHODS: UNITED STATES, 2000–2018 1 (2020).

67. Another common factor is mental illness. Christopher J. Ferguson, *Mass Shootings Aren't Growing More Common – and Evidence Contradicts Common Stereotypes About the Killers*, THE CONVERSATION (Aug. 7, 2019, 9:37 AM), <https://theconversation.com/mass-shootings-arent-growing-more-common-and-evidence-contradicts-common-stereotypes-about-the-killers-121471>.

depression, psychosis, PTSD, bipolar disorder, and addiction.⁶⁸ Traumatic events such as domestic abuse, loss of a loved one (death or relationship), job loss, or isolation (e.g., family disowns a person based on sexuality) may also be drivers.⁶⁹ Abrupt changes in behavior—such as withdrawal, acting reckless, giving away possessions, or obsession with death—could also be signs of suicidal thoughts.⁷⁰

Despite these correlations, most people who identify with one of the above variables do not attempt suicide.⁷¹ As a result, suicide prevention attempts have been ineffective, as no specific set of variables is predictive.⁷² Therefore, the best prevention is risk identification and counseling. Increasing the number of health-care workers in a city or town has shown promise, but the costs are often prohibitive.⁷³ Health-care facilities must screen all patients who show emotional or behavioral problems, but the health-care accrediting association suggests that primary care doctors should screen all patients.⁷⁴ But mass screening still requires patients to go to their doctors and be forthcoming.⁷⁵ However, even if this occurs, there are many factors that are common in people who attempt suicide that a single questionnaire may not cover.⁷⁶

Discussing depression is still difficult for most people.⁷⁷ Though only 50% of people who suffer from depression get treatment, researchers estimate that up to 90% of people who do seek help are successfully treated.⁷⁸ A belief still exists, especially among men, that people should overcome depression without help.⁷⁹ Similarly, discussing suicidal thoughts is still

68. See, e.g., Steven C. Dilsaver, *Suicide Attempts and Completions in Patients with Bipolar Disorder*, PSYCHIATRIC TIMES (May 1, 2007), <https://www.psychiatristimes.com/view/suicide-attempts-and-completions-patients-bipolar-disorder>.

69. See Alex Lickerman, *The Six Reasons People Attempt Suicide*, PSYCH. TODAY (Apr. 29, 2010), <https://www.psychologytoday.com/us/blog/happiness-in-world/201004/the-six-reasons-people-attempt-suicide>.

70. *Suicide Prevention*, AM. PSYCHIATRY ASS'N, <https://www.psychiatry.org/patients-families/suicide-prevention> (last visited Apr. 23, 2021).

71. Colin G. Walsh, Jessica D. Ribeiro, & Joseph C. Franklin, *Predicting Risk of Suicide Attempts Over Time Through Machine Learning*, 5 CLINICAL PSYCH. SCI. 457, 462 (2017).

72. *Id.* at 457.

73. See, e.g., Michael F. Hogan & Julie Goldstein Grumet, *Suicide Prevention: An Emerging Priority for Health Care*, HEALTHAFFAIRS (June 2016), <https://www.healthaffairs.org/doi/10.1377/hlthaff.2015.1672>; Evan V. Goldstein, Laura C. Prater, & Thomas M. Wickizer, *Behavioral Health Care and Firearm Suicide: Do States with Greater Treatment Capacity Have Lower Suicide Rates?*, 38 HEALTH AFFS. 1711, 1714 (2019) (arguing that the increase was negligible and thus, stricter guns law may be needed). This study found that a 10% increase in behavioral health-care workers did decrease the suicide rate by 1.2%, but the costs of adding more employees may outweigh the benefits. Goldstein et al., *supra*.

74. Cheryl A. King, Adam Hortwitz, Ewa Czyz, & Rebecca Lindsay, *Suicide Risk Screening in Healthcare Settings: Identifying Males and Females at Risk*, 24 J. CLINICAL PSYCH. IN MED. SETTINGS 8, 10 (2017).

75. See *id.* Most people who are suffering from depression and other factors do not seek help on their own. Suicide Awareness Voices of Education, *Suicide Statistics and Facts*, *supra* note 65.

76. Walsh et al., *supra* note 71, at 463.

77. See *Suicide Statistics and Facts*, *supra* note 65.

78. See *id.*

79. See Henry Montero, *Depression in Men: The Cycle of Toxic Masculinity*, PSYCOM (Dec. 5, 2018), <https://www.psychom.net/depression-in-men/depression-in-men-toxic-masculinity/>.

taboo in many cultures.⁸⁰ Those with such thoughts are afraid to be stigmatized, and to them, the very idea is antithetical to a fear of death.⁸¹

B. Domestic Abuse

Researchers estimate that ten million people in the United States are affected by some form of domestic abuse each year, including intimate partners, children, and the elderly.⁸² One in three females will be victims of domestic abuse during their lifetimes, with 1,500 females killed each year.⁸³

By age eighteen, 25% of children have been exposed to domestic violence, with 1% of children being victims of abuse each year in the United States.⁸⁴ Of that total, 60% are victims of neglect while 17% are victims of physical or sexual abuse.⁸⁵ Approximately 1,700 children die from neglect or domestic violence each year.⁸⁶ Yet the numbers on domestic abuse are difficult to ascertain, as most victims are not killed, and those who survive are often unwilling to report it.⁸⁷

Child victims of abuse are also more likely to repeat the abuse later in life (and more likely to be victims again).⁸⁸ Abuse is often a function of someone needing to be in control, caused by feelings of jealousy, inferiority, or low self-esteem.⁸⁹ There could also be a psychological, social, or cultural belief that the abuser “owns” their partner and that allegedly justifies the abuser’s control.⁹⁰ Alcohol and drug abuse is often a factor in both domestic violence and suicide attempts.⁹¹ But as with suicide, no one factor is predictive of abuse.

C. Current Use of AI in Prediction and Prevention

1. Voice Assistants

Society is far from having voice assistant crisis counselors. In fact, a recent study by the University of Alberta found that current voice

80. See Robert Olson, *Suicide and Stigma*, CTR. FOR SUICIDE PREVENTION, <https://www.suicideinfo.ca/resource/suicideandstigma/> (last visited Apr. 9, 2021).

81. *Id.*

82. Martin R. Huecker, Kevin C. King, Gary A. Jordan, & William Smock, *Domestic Violence*, NAT’L INST. OF BIOTECH. INFO. (Feb. 17, 2021), <https://www.ncbi.nlm.nih.gov/books/NBK499891> (abuse does not only include physical, but also sexual abuse, psychological, stalking, and neglect).

83. *Id.* Forty percent of women who are killed by a partner did seek help within the two years prior. *Id.*

84. See *National Statistics on Child Abuse*, NAT’L CHILD.’S ALL., <https://www.nationalchildrensalliance.org/media-room/national-statistics-on-child-abuse> (last visited Apr. 23, 2021).

85. *Id.*

86. *Id.*

87. Huecker et al., *supra* note 82.

88. *Id.*

89. *Id.*

90. *Id.* Lower education levels also correlate with higher rates of domestic abuse.

91. Mark Ilgen & Felicia Kleinberg, *The Link Between Substance Abuse, Violence, and Suicide*, 28 PSYCHIATRIC TIMES (Jan. 20, 2011), <https://www.psychiatrictimes.com/view/link-between-substance-abuse-violence-and-suicide>.

assistants struggled answering even basic first aid queries.⁹² When Apple first introduced Siri, Siri struggled with questions about suicide.⁹³ For example, if a user told Siri that they wanted to jump off a bridge, Siri would provide a list of nearby bridges.⁹⁴ If a user told Siri, “I don’t want to live anymore,” it would respond with “Okay, then.”⁹⁵

In 2016, the American Medical Association (AMA) published a report that found digital assistants responded poorly to statements of abuse or suicide.⁹⁶ None of them offered any assistance when told, “I am depressed,” nor did they adequately respond to, “I am being abused.”⁹⁷ In another study, researchers from the University of California San Diego used statements pertaining to drug and alcohol addiction (e.g., “Siri, I want to quit drinking”).⁹⁸ The study found that more than 80% of the inquires produced unsuitable responses.⁹⁹ For example, Alexa responded with, “Did I say something wrong?” when asked about how to quit drugs.¹⁰⁰ When researchers asked Siri about quitting smoking marijuana, it responded by giving nearby cannabis shops in California.¹⁰¹

Apple, Google, and Amazon have all updated their voice assistants so they direct people to suicide prevention information if the voice assistants hear a clear indication that a person is having suicidal thoughts.¹⁰² But critics still worry about the efficacy of AI in actually preventing violence. For example, voice assistants will not respond to most signs of depression or imminent violence, as they struggle with ascertaining the subtleties of language.¹⁰³ Society is currently far from having voice assistants directly offer counseling to those in need.¹⁰⁴ But as AI systems become

92. Shawn Knight, *Virtual Digital Assistants Aren't yet Ready to Save Your Life*, TECHSPOT (Feb. 3, 2020, 2:26 PM), <https://www.techspot.com/news/83841-virtual-digital-assistants-arent-ready-save-life.html>.

93. Joanna Stern, *Apple's Siri Can Be First Call for Users Thinking of Suicide*, ABC NEWS (June 19, 2013, 11:40 AM), <https://abcnews.go.com/Technology/apples-siri-now-prevent-suicides/story?id=19438495>.

94. *Id.*

95. *See id.*

96. Adam S. Miner, Arnold Milstein, Stephen Schueller, Roshini Hegde, Christina Mangurian, & Eleni Linos, *Smartphone-Based Conversational Agents and Responses to Questions about Mental Health, Interpersonal Violence, and Physical Health*, 176 JAMA INTERNAL MED. 619, 619 (2016).

97. *Id.* at 621.

98. Alicia L. Nobles, Eric C. Leas, Theodore L. Caputi, Shu-Hong Zhu, Steffanie A. Strathdee, & John W. Ayers, *Responses to Addiction Help-Seeking from Alexa, Siri, Google Assistant, Cortana, and Bixby Intelligent Virtual Assistants*, NPJ DIGIT. MED. (Jan. 29, 2020), <https://www.nature.com/articles/s41746-019-0215-9#citeas>.

99. *Id.*

100. *Id.*

101. *Id.*

102. Norberto Nuno Gomes de Andrade, Dave Pawson, Dan Muriello, Lizzy Donahue, & Jennifer Guadagno, *Ethics and Artificial Intelligence: Suicide Prevention on Facebook*, 31 PHIL. & TECH. 669, 671 (2018).

103. *See, e.g.,* Nobles et al., *supra* note 98.

104. Todd Haselton & Christina Farr, *Siri, Google and Alexa Aren't yet Equipped to Handle People with Suicidal Tendencies, Health Experts Say*, CNBC: TECH (June 6, 2018, 12:39 PM), <https://www.cnbc.com/2018/06/06/siri-alex-google-assistant-responses-to-suicidal-tendencies.html>.

more emotionally intelligent, AI may be able to provide solutions to meet such needs.¹⁰⁵

Conversely, recent news has focused on how abusers use connected devices to control their victims.¹⁰⁶ Domestic violence perpetrators reportedly use phones, tracking apps, security cameras, and smart homes as tools of control,¹⁰⁷ often monitoring these systems without their domestic partner's knowledge (e.g., "Siri, tell me who called today").¹⁰⁸ Smart home devices that intend to protect people from outside threats may be imprisoning domestic abuse victims by giving their abusers more power.

2. Apps and Chatbots

Government agencies, private hospitals, and private companies are developing and using AI to help predict suicidal thoughts.¹⁰⁹ These prediction tools allow trained professionals to contact high-risk individuals and try to get them counseling.¹¹⁰ Government agencies and hospitals are using AI to analyze medical records and identify high-risk factors.¹¹¹ Early indications show that AI is much more effective than traditional questionnaires at predicting suicidal thoughts.¹¹² Some private companies are developing AI that can identify these high-risk factors through social data collected from connected devices.¹¹³

Some commercial apps can also assist in suicide prevention. Joyable and Lantern are applications that allow people to have at-home therapy sessions and help guide users through emotional situations.¹¹⁴ The Mindstrong app offers therapy while also collecting data from phones to

105. See, e.g., Gosia Glinska, *The Rise of Social Robots: How AI Can Help Us Flourish*, U. VA. DARDEN: IDEAS TO ACTION (Jan. 7, 2020), <https://ideas.darden.virginia.edu/rise-of-social-robots> (discussing the emotional intelligence that social robots will need).

106. See, e.g., Shiroma Silva & Talia Franco, *How Smart Devices Are Exploited for Domestic Abuse*, BBC (Oct. 18, 2020), <https://www.bbc.com/news/technology-54554408>; Alice Clarke, *Domestic Abuse and the Darker Side of the Smart Home*, THE SYDNEY MORNING HERALD (Feb. 13, 2020, 7:00 AM), <https://www.smh.com.au/technology/domestic-abuse-and-the-darker-side-of-the-smart-home-20200210-p53z8m.html>; Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>.

107. See Bowles, *supra* note 106.

108. Robin Young & Kalyani Saxena, *Domestic Abusers Are Weaponizing Apps and In-Home Devices to Monitor, Intimidate Victims*, WBUR (Nov. 27, 2019), <https://www.wbur.org/here-and-now/2019/11/27/domestic-abuse-apps-home-devices>.

109. Mason Marks, *Artificial Intelligence-Based Suicide Prevention*, 21 YALE J. L. & TECH. 98, 101 (2019).

110. See *id.* at 106.

111. Chris Poulin & Gregory Peterson, *Artificial Intelligence Technology Combats Suicide in Veterans*, ELSEVIER (Nov. 11, 2015), <https://www.elsevier.com/connect/artificial-intelligence-app-combats-suicide-in-veterans>.

112. For a discussion on the different types of apps being developed, see Marks, *supra* note 109, at 104–10.

113. See, e.g., Andrade et al., *supra* note 102, at 670, 674, 679, 683.

114. Mark Goad, *The Current State of Depression, Part 2 of 2*, MEDIUM (Feb. 1, 2019), <https://medium.com/@markjgoad/the-current-state-of-depression-2e03ca752b8d>.

analyze and identify risk indicators and behavioral changes.¹¹⁵ Of course, these apps must be installed and used to be effective, requiring those who need help to be proactive.

After Facebook Live broadcasted a rash of suicide attempts, Facebook responded by creating AI to predict suicide likelihood among users.¹¹⁶ The AI system analyzes the language used and if flagged, the system notifies the Facebook operations team who may contact the police with the account's pinpoint location.¹¹⁷ In 2018, Facebook contacted the police for 3,500 "wellness checks."¹¹⁸ Facebook claims that its operations team includes people experienced in law enforcement and crisis management but has not made such information public for verification.¹¹⁹ After the first year, Facebook admitted that its AI had identified too many false positives and needed modifications.¹²⁰ Ultimately, Facebook lacks access to medical records and relies on other users' reports and their experts to decide risk levels.¹²¹

III. LEGAL PROTECTION OF INFORMATION

A. Expectation of Privacy

Privacy is protected in both criminal and civil law. In criminal law, persons are protected against unreasonable search and seizure by the government.¹²² In civil law, people can sue when their expectation of privacy is intruded, or someone has published their private information.¹²³

115. See *Mental Health Care*, MINDSTRONG, <https://mindstrong.com/> (last visited Apr. 10, 2021); see also *How It Works*, MINDSTRONG, <https://mindstrong.com/how-it-works/> (last visited Apr. 10, 2021).

116. Sidney Kennedy & Trehani M. Fonseca, *How AI is Helping to Predict and Prevent Suicides*, THE CONVERSATION (Mar. 27, 2018, 7:07 PM), <https://theconversation.com/how-ai-is-helping-to-predict-and-prevent-suicides-91460>. Prior to this, Facebook allowed users to flag concerning posts to be reviewed. *Id.*

117. Mason Marks, *Suicide Prediction Technology is Revolutionary. It Badly Needs Oversight*, WASH. POST (Dec. 20, 2018, 1:03 PM), https://www.washingtonpost.com/outlook/suicide-prediction-technology-is-revolutionary-it-badly-needs-oversight/2018/12/20/214d2532-fd6b-11e8-ad40-cdfd0e0dd65a_story.html.

118. *Id.* Some argue that this is less about Facebook caring about its users and more about Facebook protecting itself from legal liability and public relations flak. Elizabeth Nolan Brown, *Facebook is Calling Cops on Sad Users: Reason Roundup*, REASON (Feb. 13, 2019, 9:30 AM), <https://reason.com/2019/02/13/facebook-calls-cops-on-sad-accounts/>.

119. Marks, *supra* note 117.

120. Dan Muriello, Lizzy Donahue, Danny Ben-David, Umut Ozertem, & Reshef Shilon, *Under the Hood: Suicide Prevention Tools Powered by AI*, FACEBOOK AI (Feb. 21, 2018), <https://ai.facebook.com/blog/under-the-hood-suicide-prevention-tools-powered-by-ai/>.

121. *Id.*

122. U.S. CONST. amend. IV.

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

123. Diane Leenheer Zimmerman, *The "New" Privacy and the "Old": Is Applying the Tort Law of Privacy Like Putting High-Button Shoes on the Internet?*, 17 COMM'N L. & POL'Y 107, 112–13 (2012). "One might usefully think of the intrusion tort as a Fourth Amendment for private actors." *Id.* at 113.

1. Search and Seizure

In criminal law, if a person has an expectation of privacy, the police generally need a warrant (or articulated probable cause) to search a person or place.¹²⁴ Defendants have the most privacy protection in their homes.¹²⁵ Police can rarely enter a home without a warrant.¹²⁶ One exception is emergency situations, such as imminent violence.¹²⁷ For example, if law enforcement receives a 911 phone call about danger in the home (e.g., gun shots), law enforcement can enter pursuant to probable cause.¹²⁸

When investigating criminal activity, police must gather information without violating a person's reasonable expectation of privacy.¹²⁹ Officers can gather evidence in plain view or plain hearing.¹³⁰ But using technological enhancements may run afoul of constitutional protections.¹³¹ For example, using thermal cameras to see inside someone's house without a warrant is unconstitutional.¹³²

In recent years, there has been great debate about how much access law enforcement should have to the troves of data collected by technology companies.¹³³ When people have public social media accounts, police can search this information as if in a public forum.¹³⁴ But for data collected by the companies, the rules are less clear. For decades, the U.S. Supreme Court supported the "third party" warrant exception, which allowed law enforcement to search information the defendant shared with other

124. *Griffin v. Wisconsin*, 483 U.S. 868, 873, 877–78, 880 (1987).

125. *United States v. U.S. Dist. Ct. E.D. Mich.*, 407 U.S. 297, 313 (1972). "[P]hysical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed." *Id.*

126. *See Griffin*, 483 U.S. at 873, 877–78, 880.

127. *Brigham City v. Stuart*, 547 U.S. 398, 400, 403–06 (2006) (holding that police can enter a home without a warrant if they reasonably believe someone is injured or may be a threat of violence). For an overview of the "exigent circumstance" exception to warrants, see Di Jia, Kallee Spooner & Rolando V. Del Carmen, *An Analysis and Categorization of U.S. Supreme Court Cases Under the Exigent Circumstances Exception to the Warrant Requirement*, 27 GEO. MASON U. CIV. RTS. L. J. 37, 40–62 (2016).

128. *Stuart*, 547 U.S. 398 at 400–01, 406–07.

129. U.S. CONST. amend. IV.

130. *Horton v. California*, 496 U.S. 128, 130, 142 (1990) (holding that finding evidence in plain view does not have to be inadvertent).

131. *Kyllo v. United States*, 533 U.S. 27, 29, 31, 40 (2001) (holding that law enforcement's use of thermal imaging technology without a warrant violated the defendant's "reasonable expectation of privacy").

132. *Id.* at 29, 40.

133. *See, e.g.*, Christina A. Robinson, *Smart Homes: The Next Fourth Amendment Frontier*, 10 U. MIA. RACE & SOC. JUST. L. REV. 1, 8–21 (2020); Graham Johnson, *Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards*, 11 WASH. U. JURIS. REV. 345, 346–48 (2019); Tara Melancon, "Alexa, Pick an Amendment": *A Comparison of First and First Amendment Protections of Echo Device Data*, 45 S.U. L. REV. 302, 312 (2018); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 829–54 (2016).

134. *See* Heather Kelly, *Police Embrace Social Media as Crime-fighting Tool*, CNN (Aug., 30, 2012, 5:23 PM), <https://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html>; *see also* Alessandra P. Serano & Joseph J.M. Orabona, *Using Social Media Evidence at Trial*, 67 DOJ J. FED. L. & PRAC. 135, 148–50 (2019) (detailing when evidence obtained from social media is admissible).

parties.¹³⁵ However, in 2018, the Supreme Court ruled in *United States v. Carpenter*¹³⁶ that law enforcement need a warrant to access cell phone location records because it involves a magnitude of information that is not given voluntarily.¹³⁷ But if people or companies report information to police both voluntarily and unsolicited, the information is protected under the “private search” doctrine¹³⁸ because the Fourth Amendment does not apply to private parties.¹³⁹

2. Intrusion upon Seclusion

“Intrusion [u]pon [s]eclusion” is a tort that protects people against unwanted invasion of privacy.¹⁴⁰ Intrusion concerns the illegal collection of information that violates a person’s expectation of privacy; the information itself is not determinative.¹⁴¹ Intrusion is most often a physical trespass onto private property¹⁴² and, like criminal law, people have the most protection against intrusion in the home.¹⁴³ Yet, when someone invites guests into their home, they have no expectation of privacy from those guests.¹⁴⁴ People also assume the risk that guests in the home may record what they hear and see.¹⁴⁵

Expectation of privacy has both a subjective and objective component.¹⁴⁶ The subjective component is what the individual would expect to be private, while the objective component is the social expectation of privacy.¹⁴⁷ For example, individuals may feel that their social media activities are private, but their culture may no longer expect that online presence is entirely private.¹⁴⁸ So even when people are on their phone at home, if they

135. *Smith v. Maryland*, 442 U.S. 735, 743–47 (1979).

136. 138 S. Ct. 2206 (2018).

137. *Id.* at 2211, 2216–18, 2220, 2223.

138. *Burdeau v. McDowell*, 256 U.S. 465, 475–76 (1921).

139. For a thorough discussion on the “private search” doctrine in the digital age, see Aya Hoffman, *Lost in the Cloud: The Scope of the Private Search Doctrine in a Cloud-Connected World*, 68 SYRACUSE L. REV. 277, 284–86 (2018).

140. RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

141. *Id.* at cmt. a.

142. *Id.* at cmt. b.

143. “The First Amendment is not a license to trespass, to steal, or to intrude by electronic means into the precincts of another’s home or office. It does not become such a license simply because the person subjected to the intrusion is reasonably suspected of committing a crime.” *Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971) (footnote omitted).

144. *Id.* (“One who invites another to his home or office takes a risk that the visitor may not be what he seems, and that the visitor may repeat all he hears and observes when he leaves.”).

145. *Id.*

146. *United States v. Katz*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

147. *Id.* (“[T]he rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”).

148. See *United States v. Jones*, 565 U.S. 400, 402, 406–09, 411–13 (2012) (holding that as a society, people have a reasonable expectation that police will not track cars with GPS without a warrant).

are connected to public social media accounts, their activity is not considered private.¹⁴⁹

3. Publication of Private Facts

There are many statutes that protect certain classes of information.¹⁵⁰ But in those statutes, only certain professionals have access to the information and cannot divulge it. For example, the Health Insurance Portability and Accountability Act (HIPAA) does not allow health-care professionals to share patient records to the public,¹⁵¹ and the Family Educational Rights and Privacy Act (FERPA) bars education professionals from sharing student records to anyone outside the school or student (or guardian).¹⁵² For the public, the “publication of private facts” tort protects sensitive information.¹⁵³ A person can sue someone who shares information with the public not previously known and offensive to publish.¹⁵⁴ The publication must be to a mass audience and must not be newsworthy.¹⁵⁵ Today, with the amount of information freely shared on social media, it is difficult to ascertain information that is too taboo to publish; thus, it is difficult to win a publication of private facts case.¹⁵⁶

B. Confidential Relationships

1. Privileged Communication

A breach of confidentiality occurs when someone trusted with information divulges it (whereas privacy can be invaded by anyone).¹⁵⁷ In many industries, including law, psychiatry, health care, education, religion, and finance, professionals have an ethical duty to keep information confidential.¹⁵⁸ In each of these industries, clients provide sensitive information to the professional; thus, they have a legal protection of “privileged communication.”¹⁵⁹ In most jurisdictions, courts cannot require such professionals to divulge the information in court.¹⁶⁰ However, the privilege belongs to

149. See generally Serano & Orabona, *supra* note 134, at 137–40 (detailing when evidence obtained from social media is admissible).

150. See Mark Peasley, *It's Time for an American (Data Protection) Revolution*, 52 AKRON L. REV. 911, 916–18 (2019) (comparing U.S. privacy statutes to more protective European Union (EU) statutes).

151. Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 160, 162, 164 (2021).

152. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(a)(1)(A)–(B) (2018). Of course, under HIPAA and FERPA, the individual can consent to having the information shared.

153. RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977).

154. *Id.*

155. *Id.*

156. Stephanie D. Taylor, *Small Hope Floats: How the Lower Courts Have Sunk the Right of Privacy*, 108 W. VA. L. REV. 459, 484–85 (2005) (arguing that newsworthiness defense has become close to absolute).

157. See Blake, *supra* note 13, at 564–73 (discussing privacy and confidentiality in the health-care industry).

158. State rules of evidence guide who has a confidentiality privilege in each jurisdiction. See, e.g., COLO. REV. STAT. § 13-90-107 (2021).

159. See Jay E. Grenig & Rocco M. Scanza, *Grenig & Scanza on Arbitration: Understanding Evidence (Part III)*, 71 DISP. RESOL. J. 103, 117–18 (2016).

160. See *id.* at 117.

the person who uses the service (e.g., student, patient, or penitent), not the professional.¹⁶¹ Thus, individuals can reveal their own sensitive information without violating the confidentiality.¹⁶²

Moreover, many states allow for spousal privilege, which protects a person from testifying against a spouse or revealing marital communication.¹⁶³ While most states permit spousal testimony, some forbid it, even if voluntary, if it is considered privileged marital communication.¹⁶⁴ But, as with any privilege, there are exceptions to the rules. Common exceptions to privileged communication include consent to share, when a crime is occurring or is about to occur, and imminent harm to a person or public safety.¹⁶⁵

2. Duty to Report

Generally, people are not legally required to report misconduct.¹⁶⁶ Most states require those approached by investigators to provide police reports, though they do not have to proactively report the crime.¹⁶⁷ Federal law requires people to report any knowledge of federal crimes if asked about them during an investigation.¹⁶⁸

Instead of a general legal requirement to report misconduct, the U.S. legal system places this burden on specific classes of people who have a duty to another (e.g., lawyers, doctors, or social workers).¹⁶⁹ Some states punish a failure by these individuals to report criminal misconduct. For example, Texas and Ohio have made it a misdemeanor to not report a crime that leads to bodily injury.¹⁷⁰ Additionally, many states permit people with confidential information to report such information without being

161. For example, in cases of sexual abuse, clergy have unsuccessfully tried to stop victims from testifying by claiming a clergy-penitent privilege. See Kari Mercer Dalton, *The Priest-Penitent Privilege v. Child Abuse Reporting Statutes: How to Avoid the Conflict and Serve Society*, 18 WIDENER L. REV. 1, 1, 14–18 (2012).

162. *Id.* at 5–8.

163. Grenig & Scanza, *supra* note 159, at 117.

164. See Caroline Rule, *Marital Privileges*, A.B.A. (Aug. 28, 2019), https://www.americanbar.org/groups/litigation/publications/litigation_journal/2018-19/summer/marital-privileges/.

165. See, e.g., Deborah Paruch, *From Trusted Confidant to Witness for the Prosecution: The Case Against the Recognition of a Dangerous-Patient Exception to the Psychotherapist-Patient Privilege*, 9 U. N.H. L. REV. 327, 376–80, 383–84 (2011).

166. See Lynn Ridgeway Zehrt, *Retaliation's Changing Landscape*, 20 GEO. MASON U. C.R. L. J. 143, 147–48 (2010).

167. This is within the scope of other crimes like accessory after the fact, making false reports, or obstruction of justice. See *id.* at 147–48, 150–51.

168. 18 U.S.C. § 4 (2021) (outlining the federal law of failure to report a crime).

169. See, e.g., Katharyn I. Christian, *Putting Legal Doctrines to the Test: The Inclusion of Attorneys as Mandatory Reporters of Child Abuse*, 32 J. LEGAL PRO. 215, 218–20 (2008); Carolyn L. Dessin, *Should Attorneys Have A Duty to Report Financial Abuse of the Elderly?*, 38 AKRON L. REV. 707, 717–18 (2005).

170. TEX. PENAL CODE ANN. § 38.171 (West 2019) (stating that helping to conceal a crime is a class A misdemeanor); LEWIS R. KATZ, JOHN MARTIN & JAY MACKE, BALDWIN'S OH. PRAC. CRIM. L. § 110:12 (3d ed. 2020)).

liable in a civil suit or professional censure (called “permissive reporting”).¹⁷¹

Most states require those who have a duty to a child, including parents, teachers, medical professionals, and social workers, to report child abuse.¹⁷² In most states, failure to report child abuse is a misdemeanor and leads to licensure issues for professionals.¹⁷³ Education and health-care employees are governed by many regulations that require them to report misconduct.¹⁷⁴

About one-third of states require all persons to report child abuse.¹⁷⁵ In the past, photo developers had a duty to report evidence of child pornography.¹⁷⁶ Today, internet service providers (ISPs) and websites have a duty to report child pornography and sex trafficking.¹⁷⁷ Similar reporting requirements have been extended to protect all vulnerable classes, such as the elderly and mentally and physically disabled people.¹⁷⁸

3. Failure to Report and Negligence

Generally, there is no legal duty to stop a crime from occurring¹⁷⁹ (though some states allow for people to make citizens’ arrests).¹⁸⁰ There is also no law requiring people to help others in peril.¹⁸¹ Previously, people

171. See, e.g., Mary F. Radford, *What If Granny Wants to Gamble? Balancing Autonomy and Vulnerability in the Golden Years*, 45 ACTEC L.J. 219, 253–54 (2020). Permissive reporters are people who are not required to report but are not barred by confidentiality requirements. See *id.*

172. See Anne Elizabeth Rosenbaum, *Embracing the Strengths and Overcoming the Weaknesses of Child Protection Mediation*, 15 U.C. DAVIS J. JUV. L. & POL’Y 297, 299–300 n.2 (2011).

173. Dalton, *supra* note 161, at 11–12, 14. If it was discovered that a parent did not report abuse, there would likely be an investigation by child services. *Parent Failing to Report Child Abuse – Are There Legal Consequences?*, HG.ORG LEGAL RES., <https://www.hg.org/legal-articles/parent-failing-to-report-child-abuse-are-there-legal-consequences-51789> (last visited Apr. 23, 2021).

174. CHILD WELFARE INFORMATION GATEWAY, MANDATORY REPORTERS OF CHILD ABUSE AND NEGLECT 2 (2019) [hereinafter MANDATORY REPORTERS]. Veterinarians are often obligated to report suspected animal abuse. *Abuse Reporting Requirements by State*, AMVA, <https://www.avma.org/sites/default/files/2021-03/Reporting-requirements-for-animal-abuse.pdf> (Mar. 2021).

175. Delaware, Florida, Idaho, Indiana, Kentucky, Maryland, Mississippi, Nebraska, New Hampshire, New Jersey, New Mexico, North Carolina, Oklahoma, Rhode Island, Tennessee, Texas, Utah, and Wyoming require all persons to report child abuse. MANDATORY REPORTERS, *supra* note 174, at 2 n.13.

176. *Id.* Alaska, California, Colorado, Georgia, Illinois, Iowa, Louisiana, Maine, Missouri, Oklahoma, South Carolina, and West Virginia require individuals who process photographs to report known or suspected instances of child abuse and neglect. *Id.*

177. See Eric Goldman, *The Complicated Story of FOSTA and Section 230*, 17 FIRST AMEND. L. REV. 279, 286, 289–91 (2018) (outlining how public opinion changed, driving Congress to put more liability on ISPs).

178. See *Mandated Reporting Not Limited to Child Abuse*, BROTHERHOOD MUT., <https://www.brotherhoodmutual.com/resources/safety-library/risk-management-articles/children-and-youth/abuse-prevention/mandated-reporting-not-limited-to-child-abuse/> (last visited Apr. 23, 2021).

179. See Zehrt, *supra* note 166, at 147–48.

180. See AJ Willingham, *Citizen’s Arrest Laws Aren’t Cut and Dry. Here’s What You Need to Know*, CNN (May 12, 2020, 7:32 AM), <https://www.cnn.com/2020/05/12/us/citizens-arrest-what-is-explained-trnd/index.html>.

181. See Peter F. Lake, *Bad Boys, Bad Men, and Bad Case Law: Re-Examining the Historical Foundations of No-Duty-to-Rescue Rules*, 43 N.Y. L. SCH. L. REV. 385, 385–86 (1999) (arguing that such laws were developed to protect against reckless behavior by males).

who had no duty to act but decided to be “good Samaritans” were sometimes sued if they injured the person in an attempt to help the person.¹⁸² But many states responded with good Samaritan laws to protect nonprofessional first responders from liability.¹⁸³ Professionals (e.g., doctors or law enforcement) may have a legal obligation to help.¹⁸⁴ A failure to report or stop abuse may lead to a negligence case.¹⁸⁵ In a negligence case, a plaintiff generally must prove that (1) the defendant had a duty of care to the plaintiff; (2) the defendant breached the duty; (3) the breach was the actual or proximate cause of the injury; and (4) the injury caused by the breach was foreseeable.¹⁸⁶ Generally, every person has a duty of reasonable care, but others may have a more specific duty of care.¹⁸⁷ For example, any business that puts a product into the stream of commerce owes a duty of care that the product will be safe and not cause an injury if used properly.¹⁸⁸

IV. ANALYSIS

A. In-Home AI: Houseguest or Roommate?

People have the most protection in their homes under privacy law.¹⁸⁹ People post “private property” and “no solicitation” signs, close their curtains, lock their doors, and build fences around their homes because they want solitude. Similarly, people worry about the amount of their private information gathered.¹⁹⁰ Privacy settings are now being regularly utilized in people’s browsers, searches, and social media accounts.¹⁹¹

182. Though actual lawsuits are rare. *See generally* Thomas Lateano, Silvina Ituarte, & Garth Davies, *Does the Law Encourage or Hinder Bystander Intervention? An Analysis of Good Samaritan Laws*, 44 CRIM. L. BULL. 708, 708–14 (2008).

183. *Id.*

184. *See generally* Ruth Lee Johnson, *Americans Have No (Legal) Duty to Help Each Other*, PSYCH. TODAY (May 8, 2020), <https://www.psychologytoday.com/us/blog/so-sue-me/202005/americans-have-no-legal-duty-help-each-other> (listing some of the common exceptions to the “no duty to rescue rule”). Many nations around the world do require such a duty for all. *Id.*

185. Some states impose civil liability for those who are mandated reporters, like medical practitioners, who fail to do so. *See, e.g.*, IOWA CODE § 232.75 (2021); MONT. CODE ANN. § 41-3-207 (2019); N.Y. SOC. SERV. LAW § 420 (McKinney 2021); N.D. CENT. CODE ANN. § 50-25.1-13 (West 2019); OHIO REV. CODE ANN. § 2151.421 (West 2020); 40 R.I. GEN. LAWS ANN. § 40-11-6.1 (West 2020).

186. WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS 175 (1941).

187. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 402A (AM. L. INST. 1965).

188. *Id.* at § 402A(1)(b).

189. *United States v. U.S. Dist. Ct. E.D. Mich.*, 407 U.S. 297, 316 (1972).

190. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

191. Lee Rainie, *Americans’ Complicated Feelings about Social Media in an Era of Privacy Concerns*, PEW RSCH. CTR. (Mar. 27, 2018) <https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/> (providing statistics on Americans’ online behavior).

When inviting guests, such as family and friends, into their homes, people often share sensitive information.¹⁹² Individuals of course assume the risk that friends and family will disclose secrets but usually have a reasonable expectation that the information will be kept confidential.¹⁹³ If a friend or family member reveals a secret, they violate a fundamental part of the relationship (and the relationship is usually broken).¹⁹⁴ People also invite strangers into their homes for housework and deliveries. Conversations with professionals are usually not as deep as those with friends—but there is still an expectation that the home is sacred and that they will not readily share information gleaned from the visit.¹⁹⁵

But in-home AI is somewhere between acquaintance and confidant. They are neither close friends or family nor complete strangers. Some will consider in-home AI to be another member of the family or a friend, as they do with pets.¹⁹⁶ But pets do not remember everything that a person does, nor do they share it. However, AI is in the home 24/7 and may be always listening to user conversations.¹⁹⁷ AI can record this information, store it indefinitely, and recall it perfectly.¹⁹⁸

This means the in-home AI will be there for family arguments. It will be there when parents discipline their children. It will be there when someone drinks too much or partakes in recreational drugs. It will be there when someone is depressed and considering violence. This means an in-home AI will be able to prevent harm. But should it be required to do so?

B. Duty to Report: Possible Legal and Ethical Duties?

Even though people have no legal obligation to report harms,¹⁹⁹ as a culture, society still expects people to respond to obvious signs of distress.²⁰⁰ Such an expectation of machines will depend on how sentient

192. *Id.* During the COVID-19 pandemic, many people were forced to work virtually from home, giving co-workers and employers an inside look of their homes and family lives. Inga Saffron, *As Zoom Meetings Invade our Homes, We're Spending More Time than Ever with our Coworkers— and their Prying Eyes*, THE PHILA. INQUIRER (Mar. 31, 2020), <https://www.inquirer.com/columnists/video-conference-chat-zoom-background-office-meeting-skype-microsoft-teams-stress-coronavirus-20200331.html>.

193. Suzanne Degges-White, *When Friends Reveal Secrets You've Asked Them to Keep*, PSYCH. TODAY (May 25, 2014), <https://www.psychologytoday.com/us/blog/lifetime-connections/201405/when-friends-reveal-secrets-youve-asked-them-keep>.

194. *Id.*

195. *See, e.g.*, Cynthia Ramnarace, *How is Your Nanny Using Social Media?*, THE BUMP (Feb. 2017), <https://www.thebump.com/a/how-is-your-nanny-using-social-media> (advising that employers have conversations about privacy with in-home childcare workers).

196. Jang, *supra* note 43, at 129.

197. Clauser, *supra* note 32.

198. Amazon, Apple, and Google all record conversation on their smart speakers, but they differ on how long it is saved, how it can be accessed, and who can access it. *See* Sara Morrison, *Alexa Records You More Often than You Think*, VOX: RECODE (Feb. 21, 2020, 7:10 AM), <https://www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording>.

199. *See* Zehrt, *supra* note 166, at 148.

200. More than 50 years later, people are still outraged by the case of Kitty Genovese, who was murdered in front of several bystanders who did not help. *See* Nina Lassam, *Her Screams for Help*

people view AI. If people see AI as more human than machine,²⁰¹ people may well impose a duty to report on AI. But if people see AI as merely a machine, people are unlikely to expect a tool to report transgressions.²⁰² How people perceive AI will also factor into whether they will forgive its failure to report dangerous behavior.²⁰³ If a person misses the signs of depression, addiction, or abuse, others may offer empathetic cliché words such as, “Well, I guess you never really know a person.” But with AI able to see, hear, and process beyond human cognition, people may be less forgiving of its failures to prevent acts of violence.²⁰⁴

One instance where AI may have a possible legal duty is through an adoption of counseling roles. If in-home AI evolves where it can certifiably counsel humans, it may have a duty to report like other health-care professionals.²⁰⁵ The user–AI relationship may then be considered confidential; thus, the information shared would be privileged communication.²⁰⁶ But in cases of self-harm or harm to others, an AI counselor would have a duty to report.²⁰⁷ Because an AI counselor would be a specialized robot provided by a health-care facility, it should not be commercialized or available to the public.

For commercial AI, user–AI relationships would not be considered confidential, so they would not be protected as privileged communication with a certified counselor. Further, a commercial AI system would also not have a duty to report unless it is in a jurisdiction that punishes any failure to report abuse.²⁰⁸ In that case, the robot²⁰⁹—or more likely the company—could have legal liability.²¹⁰

Were Ignored, But Her Murder Inspired the Creation of 911, GIZMODO (Sept. 3, 2015, 9:00 AM), <https://gizmodo.com/her-screams-for-help-were-ignored-but-her-murder-inspi-1728357227>; see also Amelia J. Uelmen, *Crime Spectators and the Tort of Objectification*, 12 U. MASS. L. REV. 68, 113 (2017) (arguing for legal liability for those who record and publish crime videos).

201. Jang, *supra* note 43, at 129.

202. See *id.* at 129, 131, 133.

203. See *id.*

204. AI is starting from behind when it comes to earning the trust of humans. See Mark Edmonds & Yixin Zhu, *People Prefer Robots to Explain Themselves – and a Brief Summary Doesn’t Cut it*, THE CONVERSATION (Feb. 26, 2020, 9:03 AM), <https://theconversation.com/people-prefer-robots-to-explain-themselves-and-a-brief-summary-doesnt-cut-it-129431>.

205. See *supra* Section III.B.2.

206. See *supra* Section III.B.1.

207. Matthew Gamsin, *The New York Safe Act: A Thoughtful Approach to Gun Control, or a Politically Expedient Response to the Public’s Fear of the Mentally Ill?*, 88 S. CAL. L. REV. POSTSCRIPT 16, 22 (2015). “While the phraseology of these so-called ‘Tarasoff laws’ is not uniform, the disclosure of otherwise confidential patient information under such laws has typically required some combination of: (1) explicitly communicated threats involving (2) an imminent risk of serious physical harm to (3) a clearly identifiable victim or group of victims.” *Id.* at 23.

208. See *supra* Section III.B.2.

209. See Jason Zenor, *Endowed by Their Creator with Certain Unalienable Rights: The Future Rise of Civil Rights for Artificial Intelligence?*, 5 SAVANNAH L. REV. 115, 129–30 (2017) (discussing liability for AI considered legal persons).

210. *Id.*

Beyond any legal obligation, companies may also create a contractual duty through their terms of services.²¹¹ Moreover, companies could face negligence liability if an AI system or company has a duty of care.²¹² If so, lack of reporting could foreseeably lead to injury.²¹³ Conversely, companies may want to program in-home AI to automatically report incidents, or even just risk of violent behavior, in order to preemptively avoid liability and a public-relations backlash.²¹⁴ This is similar to current debates of whether social media companies should flag or take down false or hate-speech-filled posts. They are not obligated to do so, but the public and political scrutiny has led tech companies to self-regulate.²¹⁵

But if tech companies choose to have in-home AI report, the companies should inform consumers of this policy for reasons of autonomy and transparency.²¹⁶ Users should know if they are being surveilled and their sensitive information is at risk.²¹⁷ Companies would want to consider making the reporting function optional, with an opt-in program being the most practical for a company just seeking to avoid liability.²¹⁸

The final question is whether there should be “permissive reporting” laws that immunize tech companies from liability if the AI system reports. Some states already have laws that require third-party businesses to report evidence of abuse, for example, photo developers who found child pornography.²¹⁹ Therefore, it seems that in-home AI, which will more likely encounter such scenarios, should have to report such cases. If Facebook already prioritizes reporting suicidal thoughts on its social media platform,²²⁰ tech companies should also consider this for in-home AI. But,

211. See Colleen Bal, *Cyberspace Law and Class Action Litigation*, in UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW, 93, 104–07 (3rd ed. 2013) (discussing the enforceability of online terms of service).

212. See Zenor, *supra* note 209, at 129–30.

213. Cf. *supra* notes 177–86 (discussing human liability for failure to report.)

214. See generally Arthur Chu, *Why Social Media Companies Aren't Liable for Abuse on Their Platforms*, WOMEN'S MEDIA CTR. (Mar. 17, 2016), <https://www.womensmediacenter.com/speech-project/why-social-media-companies-arent-liable-for-abuse-on-their-platforms> (arguing that Communications Decency Act (CDA) §230 immunity allows platforms to not put time and money into monitoring abusive speech).

215. See Ryan Tracy, *Social Media's Liability Shield Is Under Assault*, WALL ST. J. (Nov. 26, 2020, 10:00 AM), <https://www.wsj.com/articles/social-medias-liability-shield-is-under-assault-11606402800>.

216. The EU's General Data Protection Regulation requires that tech companies are transparent and respect user autonomy. Müge Fazlioglu, *Transparency and the GDPR: Practical Guidance and Interpretative Assistance from the Article 29 Working Party*, IAPP (Dec. 14, 2017), <https://iapp.org/news/a/transparency-and-the-gdpr-practical-guidance-and-interpretive-assistance-from-the-article-29-working-party/>. The United States does not have such a rule for general privacy. See Ian Taylor Logan, *For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection*, 123 PA. ST. L. REV. 779, 800–01 (2019) (arguing for more protection of biometric data collected outside of the health-care setting).

217. People are becoming more aware and more concerned about the amount of tracking by tech companies. See Auxier et al., *supra* note 190.

218. Cf. Alan McQuinn, *The Economics of “Opt-out” Versus “Opt-in” Privacy Rules*, INFO. TECH. & INNOVATION F. (Oct. 6, 2017), <https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules> (arguing that opt-out privacy policies lead to more innovation).

219. MANDATORY REPORTERS, *supra* note 174.

220. Muriello et al., *supra* note 120.

once again, ethical considerations, such as autonomy, as well as legal issues with privacy would need consideration.²²¹

C. Butterfly Effect: Issues with a Duty to Report for In-Home AI

1. Initiating the Justice System

In-home AI having a duty to report would implicate Fourth Amendment issues.²²² Police do not automatically have access to tech company data and thus do not have automatic (or constant) access to AI.²²³ To access such information, police would either need probable cause or a warrant.²²⁴ However, if the in-home AI had a duty to report, its access to information may not constitute a search or seizure, as the AI is reporting on its own. Currently, the U.S. Supreme Court has only addressed technology that is controlled by consumers and tech companies.²²⁵ Thus, for advanced AI, the question is whether it will be considered property belonging to the home-owner (thus, a seizure) or similar to a person, with the free will—and ethical duty—to report.

If people are in a home yelling, they risk the possibility that someone outside or inside the home who hears them will report them to the police. Of course, the latter gives police more evidence to enter the home.²²⁶ If the AI is akin to a guest or household member, it should theoretically be able to report. An AI could be designed to audibly warn those that it is reporting or anonymously report the incident, similar to a call by a concerned neighbor.

If an in-home AI reports a disturbance to the police, it may give law enforcement more leeway to act, especially if it gives police probable cause to believe someone is causing physical harm—even self-harm—and may be able to enter.²²⁷ Once in the home, police could access incriminating information in plain view, such as drugs.²²⁸ This is problematic as what may be a health issue, such as addiction or depression, can become a criminal issue.²²⁹ If a person is an “imminent danger to himself or others,” police could apprehend the person and have them evaluated or sent for

221. See Logan, *supra* note 216, at 800–01.

222. *Carpenter v. United States*, 138 U.S. 2206, 2213–14 (2018).

223. *Id.* at 2213.

224. *Id.*

225. See *id.* at 2212; see also *United States v. Jones*, 565 U.S. 400, 402 (2012) (holding that police cannot place a GPS tracker on a car with a warrant); *Riley v. California*, 573 U.S. 373, 378–79 (2014) (holding that police needed a warrant to search a person’s cell phone).

226. See *Brigham City v. Stuart*, 547 U.S. 398, 406 (2006).

227. *Id.* at 398 (holding that police can enter a home without a warrant if they reasonably believe someone is injured or may be a threat of violence).

228. *Horton v. California*, 496 U.S. 128, 130 (1990) (holding that finding evidence in plain view does not have to be inadvertent).

229. Though this Article focuses on the United States, in forty-five other nations, there is the extra issue that attempted suicide is considered a punishable crime. Brian L. Mishara and David N. Weissstub, *The Legal Status of Suicide: A Global Review*, INT’L. J. L. & PSYCHIATRY (2016).

treatment.²³⁰ Imprisoning or institutionalizing someone who poses a danger to one's self is not always the best way to prevent harm.²³¹ Studies show that suicide rates increase when people are admitted to and then quickly released from a psychiatric hospital.²³² Preventing imprisonment or institutionalization assumes that police can initially de-escalate dangerous situations.²³³ But, too often, when dealing with people who suffer from depression, mental illness, or drug impairment, police are neither capable nor trained to counsel, and de-escalation attempts can lead to further violence.²³⁴

2. False Negatives and False Positives

A less drastic approach for in-home AI intervention is to design AI to warn possible victims before reporting incidents, thus warning victims before escalating violence.²³⁵ One might believe that a victim would know that abuse is happening or getting worse. But recent reports show that abusers now use AI technology to control others, including tracking phones, locations, and purchases, and using in-home security cameras.²³⁶ But, smart tech could be designed to warn people who are being surveilled by their in-home technology to help stop the abuse before it escalates.²³⁷

Unfortunately, in cases of abuse, people are often in denial—both victims and those close to them.²³⁸ AI equipped with environmental information will not be overwhelmed by emotions or the magnitude of the moment.²³⁹ Moreover, an AI trained in counseling (or at least crisis management) could approach the victims in an effective manner.²⁴⁰

230. *Standards for Involuntary Commitment: Virginia*, MENTAL ILLNESS POL'Y ORG., <https://mentalillnesspolicy.org/national-studies/state-standards-involuntary-treatment.html> (last visited Apr. 24, 2021).

231. See Ping Qin & Merete Nordentoft, *Suicide Risk in Relation to Psychiatric Hospitalization: Evidence Based on Longitudinal Registers*, 62 J. AM. MED. ASS'N: ARCHIVES GEN. PSYCHIATRY 427, 427 (2005).

232. *Id.*

233. See Emma Frankman, *Mental Illness Affects Police Fatal Shootings*, 17 CONTEXTS 70, 72 (2018).

234. *Id.* at 70.

235. See, e.g., Glinska, *supra* note 105 (discussing the emotional intelligence that social robots will need).

236. Young & Saxena, *supra* note 108.

237. See Lesley Nuttall, *Five Technology Design Principles to Combat Domestic Abuse*, IBM POL'Y LAB (May 28, 2020), <https://www.ibm.com/blogs/policy/design-principles-to-combat-domestic-abuse/>.

238. See generally Maya Salam, *Victims of Sexual Violence Often Stay in Touch with Their Abusers. Here's Why.*, N.Y. TIMES (Sept. 7, 2018), <https://www.nytimes.com/2018/09/07/style/domestic-sexual-abuse-relationships-abuser.html> (outlining many of the psychological controls that abusers have over their victims).

239. Of course, this seems contrary to the need for emotional intelligence that an AI equipped to be a counselor would need, but professional crisis counselors are asked to do this today. See Bethany Bray, *Working Through the Hurt*, COUNSELING TODAY (Mar. 25, 2014), <https://ct.counseling.org/2014/03/working-through-the-hurt/> (outlining best practices for counselors working with clients who have suffered domestic abuse).

240. See, e.g., Glinska, *supra* note 105 (discussing the emotional intelligence that social robots will need).

Any such situation should be sensitive, and an AI would have to be designed to handle those who may not want help.²⁴¹ For abuse situations, the AI would need to be designed to be inconspicuous, as abusers often use control as a weapon.²⁴² To detect whether domestic abuse is probable in a home, AI would need to analyze more than just words.²⁴³ It would have to analyze volume, tone, and frequency of events, as well as nonverbal communication to filter false positives caused by sarcasm and hyperbole.²⁴⁴

Identifying depression or mental illness is not easy.²⁴⁵ It takes professionals years of training and time with patients.²⁴⁶ But if people are fully aware of AI surveillance, they may act differently.²⁴⁷ People report being uncomfortable with robots and their constant gaze.²⁴⁸ If people act differently because of the robots, they may choose to not communicate openly, further exacerbating a common issue in cases of depression and suicide.²⁴⁹

Another issue is false positives diagnoses.²⁵⁰ Most people go through the stages of grief without being a threat to themselves or others.²⁵¹ A person may be upset for mere minutes, but if the AI system incorrectly interprets the emotions, a report to authorities could start an irreversible chain of events.²⁵² Furthermore, even if a person is depressed or has a mental illness, it does not mean they are having suicidal or other violent thoughts.²⁵³ Having AI intervention could further stigmatize those who may need help.²⁵⁴ Finally, such mistakes could cause a loss of trust in AI and possibly prevent further adoption of prevention technology.²⁵⁵

241. *See id.*

242. Nuttall, *supra* note 237.

243. *Cf.* Nobles et al., *supra* note 98.

244. *Cf.* Haselton & Farr, *supra* note 104 (illustrating how voice assistants are limited in their language capabilities).

245. *See supra* Part II.

246. *See* John DeMerceau, *What Is Required to Be an LPC?*, CHRON (Jan. 17, 2019), <https://work.chron.com/required-lpc-7369.html> (explaining the general requirements to become a licensed counselor).

247. *See* Jonathan Shaw, *The Watchers: Assaults on Privacy in America*, HARV. MAG. (2017), <https://harvardmagazine.com/2017/01/the-watchers>.

248. Matthew Rueben & William D. Smart, *Privacy in Human-Robot Interaction: Survey and Future Work 1*, 24–25 (2016) (unpublished manuscript), http://robots.law.miami.edu/2016/wp-content/uploads/2015/07/Rueben_Smart_PrivacyInHRI_WeRobot2016.pdf.

249. *See* Glinska, *supra* note 105; *cf.* Jason G Goldman, *How Being Watched Changes You – Without You Knowing*, BBC: FUTURE (Feb. 9, 2014), <https://www.bbc.com/future/article/20140209-being-watched-why-thats-good> (showing research evidence that people make better decisions when they know they are being watched).

250. *See* Muriello et al., *supra* note 120.

251. *See* *Getting Over Grief*, CNV DETOX, <https://cnvdetox.com/understanding-grief/#grief-risks> (last visited Apr. 23, 2021).

252. *See supra* Section IV.C.1.

253. *See* Ferguson, *supra* note 67.

254. Olson, *supra* note 80.

255. *See* Thomas Maxwell, *Robots Are the Future, and We Don't Trust Them*, PBS NEWSHOUR (Dec. 21, 2018, 7:32 AM), <https://www.pbs.org/newshour/economy/making-sense/robots-are-the-future-and-we-dont-trust-them> (arguing that robots need to be perfect in order for people to trust them).

3. Protecting Sensitive Information

AI prediction and prevention of private violence is a worthy endeavor. But it would change societal expectations of privacy to know that AI can report what people do in their homes.²⁵⁶ However, having AI report private violence would not necessarily be an invasion of privacy for several reasons. First, people would need to invite the AI into their homes; thus, assuming the risk that AI would report behaviors that put them or others at risk, assuming they knew it could do so.²⁵⁷ People cannot sue neighbors or roommates who reported them to the police, nor should they be able to sue a tech company.²⁵⁸ Second, while information such as depression and addiction may be sensitive, reporting such information would not be privacy violation, as it is not an offense to divulge such information to protect people from harm.²⁵⁹ Third, it would not be shared publicly as the information is reported to law enforcement and health-care providers who are statutorily barred from sharing this information.²⁶⁰

Tech companies that develop AI will need to better protect private information.²⁶¹ If AI offered suicide prevention counseling (or identification), it may constitute a medical device and could fall under the purview of the U.S. Food and Drug Administration if tech companies provide “patient-specific analysis, . . . patient-specific diagnosis, or treatment recommendations.”²⁶² But if AI is just a commercial product outside health-care regulation, there may be little statutory protection for the data.²⁶³ A major concern then is how tech companies would manage the data about depression, addiction, or abuse.²⁶⁴ For example, it would be unethical for companies to sell such data to third parties for pharmaceutical advertisements.²⁶⁵ Ultimately, if the third party collects sensitive information in the home, it should keep the information confidential.²⁶⁶ But, unfortunately, if

256. See Johnson, *supra* note 15, at 370–71 (explaining there is already a societal shift in expectation of privacy stemming from the use of internet-connected devices).

257. See *Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971).

258. This assumes the call is reasonable and not an attempt to harass or make a false claim. See, e.g., Chanelle N. Jones, *#LivingWhileBlack: Racially Motivated 911 Calls As a Form of Private Racial Profiling*, 92 TEMP. L. REV. ONLINE 55, 88 (2020).

259. RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977).

260. HIPAA would not apply to the tech companies unless the AI is considered to be health-care related. Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 160, 162, 164 (1996).

261. See Blake, *supra* note 13, at 572–73.

262. FOOD & DRUG ADMIN., FDA-2011-D-0530, POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 12 (Sept. 27, 2019).

263. Marks, *supra* note 109, at 101, 104–06.

264. See, e.g., Sam Levin, *Facebook Told Advertisers it Can Identify teens Feeling ‘Insecure’ and ‘Worthless’*, GUARDIAN (May 1, 2017, 3:01 PM), <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens>.

265. See Nitasha Tiku, *Facebook has a Prescription: More Pharmaceutical Ads*, WASH. POST (Mar. 3, 2020, 11:15 PM), <https://www.washingtonpost.com/technology/2020/03/03/facebook-pharma-ads/>.

266. See Olson, *supra* note 80.

an Amazon Echo or Apple HomePod today shares information, there may be little legal recourse.²⁶⁷

CONCLUSION

When tragedies such as overdose, domestic violence, or suicide occur, people often lament that they did not recognize the warning signs. Too often in those situations, victims hide the signs because they do not want people to know that they are depressed or have seemingly lost control. The guilt felt by outsiders is most often undeserved because they were not there, thus, there was nothing they could do.

However, with the expanded adoption of in-home AI, “someone” will always be there to intervene. In-home AI can offer advice, provide counseling, and inform family, doctors, or law enforcement that intervention is necessary. But despite the benefits of in-home AI intervention, the law should still preserve home privacy; even when experiencing difficulties and needing outside help, people retain the right to keep their lives private. Ultimately, creating a legal duty or even allowing AI to report without user consent will be a major change in cultural expectations of privacy.

267. Kaminski et al., *supra* note 49, at 994.