

August 2025

GAI-Enabled Real Estate Fraud Schemes: Risks, Prevention and Regulations

Li Lin

Follow this and additional works at: <https://scholarship.law.ufl.edu/jtlp>

Recommended Citation

Lin, Li (2025) "GAI-Enabled Real Estate Fraud Schemes: Risks, Prevention and Regulations," *Journal of Technology Law & Policy*: Vol. 29: Iss. 1, Article 4.

Available at: <https://scholarship.law.ufl.edu/jtlp/vol29/iss1/4>

This Note is brought to you for free and open access by UF Law Scholarship Repository. It has been accepted for inclusion in *Journal of Technology Law & Policy* by an authorized editor of UF Law Scholarship Repository. For more information, please contact rachel@law.ufl.edu.

GAI-ENABLED REAL ESTATE FRAUD SCHEMES: RISKS, PREVENTION AND REGULATIONS

Li Lin*

INTRODUCTION	97
I. CONTEMPORARY GAI DEVELOPMENT AND APPLICATION IN FRAUD.....	98
A. <i>Defining AI and GAI</i>	98
B. <i>How AI and GAI Are Used in Fraud</i>	100
II. GAI-ENABLED FRAUD SCHEMES IN MODERN REAL ESTATE MARKET	103
A. <i>How GAI Can Be Used to Further Real Estate Fraud Schemes</i>	103
B. <i>Real Estate Fraud in the Growing Florida Market</i>	108
III. GAI-ENABLED FRAUD PREVENTION, REGULATIONS, AND POLICY SUGGESTIONS.....	109
A. <i>GAI-Enabled Real Estate Fraud Prevention</i>	109
B. <i>Current Real Estate Fraud Prevention Programs and Statutes</i>	110
C. <i>U.S. Regulations Regarding GAI Use in Fraud</i>	112
D. <i>Discussion</i>	114
CONCLUSION AND SUGGESTIONS	115

INTRODUCTION

The emergence of generative artificial intelligence (GAI) has posed both opportunities and challenges to our society. On the one hand, GAI drives economic growth by improving automation on the supply side and providing personalization on the demand side.¹ On the other hand, the use

* J.D. expected 2025, the University of Florida Levin College of Law; Bachelor of Laws degree from Sun Yat-sen University. I would like to express my gratitude to John Carroll, a practicing attorney in South Carolina, who inspired me to write this Note and provided exceptional guidance. Special thanks are also extended to Ceon Wong and the *Journal of Technology Law and Policy* for their insightful feedback, as well as to Professor Jiaying Jiang and Advisor Alisha Tabag for their invaluable mentorship. Finally, the author would like to thank her family, friends, and partner for their unwavering support and encouragement throughout the journey.

1. Danxia Chen et al., *Exploring Generative Artificial Intelligence (GAI): Business Professionals' Surveys and Perceptions on GAI*, 24 J. BEHAVIORAL & APPLIED MGMT. 79, 80 (2024), <https://www.semanticscholar.org/reader/413dfda358df6e360805189f93b95ec71dc6caea> [https://perma.cc/GFX5-2FX6].

of GAI raises many ethical and security concerns.² This Note focuses on how GAI can be used in real estate fraud schemes and how governments and other entities are fighting that trend. The first section of this Note discusses the contemporary development and application of GAI in fraud. The second section examines common types of GAI-enabled real estate fraud schemes and particularly their impact on the Florida real estate market. The third section explores how GAI can combat GAI-enabled fraud such as deepfake impersonation and phishing attacks and reviews the legislation and programs many states have adopted to address these issues. The fourth section digs deeper and discusses why federal and state regulations lag behind the technological advances in artificial intelligence (AI), particularly GAI. Finally, this Note concludes by analyzing the prospects of preventing GAI-enabled real estate fraud and providing policy suggestions.

I. CONTEMPORARY GAI DEVELOPMENT AND APPLICATION IN FRAUD

A. *Defining AI and GAI*

If you are an iPhone user and want to find something on your phone as fast as possible, what would you do? You would probably ask Siri, a popular AI product. Similarly, if you have difficulty answering a question posed by your professor, or are confused about the meaning of your dream last night, you would probably go to ChatGPT, one of the most popular GAI products on the market. These are all daily examples of AI and GAI use in our lives.

Indeed, the development of AI and GAI has transformed the technological landscape and impacted almost every aspect of our lives.³ The term *artificial intelligence* first appeared in 1956 when John McCarthy, a computer scientist at Stanford, hosted the eight-week-long *Dartmouth Summer Research Project on Artificial Intelligence* at Dartmouth College.⁴ There is no agreed-upon definition of AI, but an important idea beneath the creation of AI is to make machines and computers imitate human intelligence.⁵ However, AI systems are not humans. They are efficient statistical predictors of information rather than

2. Abenezer Golda et al., *Privacy and Security Concerns in Generative AI: A Comprehensive Survey*, 12 IEEE ACCESS 48126, 48126 (2024), <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10478883> [<https://perma.cc/Z8GG-F2V5>].

3. Gianluca Riccio, *2 Years of ChatGPT: How Its Impact Has Already Changed the World*, FUTURO PROSSIMO (Nov. 25, 2024), <https://en.futuroprossimo.it/2024/11/2-anni-di-chatgpt-come-il-suo-impatto-ha-gia-cambiato-il-mondo/> [<https://perma.cc/CZ4E-QLEV>].

4. Michael Haenlein & Andreas Kaplan, *A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence*, 61 CAL. MGMT. REV. 1, 3 (2019), <https://journals.sagepub.com/doi/epub/10.1177/0008125619864925> [<https://perma.cc/M558-SFGE>].

5. HAROON SHEIKH ET AL., MISSION AI: THE NEW SYSTEM TECHNOLOGY 15 (2023).

entities that possess the anthropomorphic attribute of “common sense.”⁶ Nevertheless, AI possesses its unique strength and has successfully outperformed humans in different task assignments, such as playing chess.⁷

GAI is an AI model or algorithm that generates brand-new content in response to a prompt.⁸ Unlike other forms of AI that take existing information to answer specific questions or generate new content, GAI creates new information from scratch.⁹ GAI uses a computing process known as deep learning to analyze patterns in large sets of data and then replicates the patterns to create new data that appears human-generated.¹⁰ Deep learning is a subset of machine learning models inspired by the human brain that utilizes artificial neural networks.¹¹ It comprises different layers of interconnected nodes and data flows through these layers to provide a final result or prediction.¹² GAI can generate various types of content, including text, audio, image, video, and even three-dimensional models.¹³ In December 2023, Professor Shen Yang, with the assistance of GAI, spent three hours creating a science fiction novel entitled *The Land of Machine Memories*, which won second prize in the Jiangsu Popular Science and Science Fiction Competition.¹⁴ Industry experts predict that GAI could raise global domestic product (GDP) by

6. J.E. (Hans) Korteling et al., *Human- Versus Artificial Intelligence*, 4 FRONTIERS IN A.I. 1, 3 (2021).

7. See Jon M. Garon, *Prometheus' Digital Fire: The Civic Responsibilities of Artificial Intelligence*, 20 OHIO ST. TECH. L.J. 225, 231 (2024). There are different types of AI systems classified based on task assignments. Predictive AI is a computer program's ability to use statistical analysis to identify patterns, anticipate behaviors, and predict future events. Although the predictions are not necessarily accurate, they help businesses make better decisions and personalize experiences for their customers. Automating AI refers to AI systems that automate processes within businesses or other entities, often resulting in the replacement of human workers. Extractive AI involves extracting information from existing sources, such as text summarization. Conversational AI combines Natural Language Processing (NLP) to imitate conversations with human beings. See *id.* at 233–35.

8. *Id.* at 234.

9. *Id.*

10. Megan Crouse, *Generative AI Defined: How it Works, Benefits and Dangers*, TECHREPUBLIC (Oct. 24, 2024), <https://www.techrepublic.com/article/what-is-generative-ai/> [https://perma.cc/PY9P-WLYL].

11. Faisal Kalota, *A Primer on Generative Artificial Intelligence*, EDUC. SCI. 1, 5 (2024).

12. *Id.*

13. Fiona Fui-Hoon Nah et al., *Generative AI and ChatGPT: Applications, Challenges and AI-human Collaboration*, 25 J. INF. TECH. CASE AND APP. RSCH. 277, 279 (2023), <https://www.tandfonline.com/doi/epdf/10.1080/15228053.2023.2233814?needAccess=true> [https://perma.cc/5RS9-FKKC].

14. Garon, *supra* note 7, at 235.

7% and replace 300 million jobs of knowledge workers.¹⁵ In this Note, both terms *AI* and *GAI* are used and discussed, but *GAI* is the main focus of this Note.

B. How AI and GAI Are Used in Fraud

Fraud exists in all walks of life, and detecting and preventing fraud is relevant to many stakeholders in society. With the rise of AI and GAI, new opportunities have emerged to detect and prevent fraud.¹⁶ However, fraudsters also leverage AI to commit fraud and crimes.¹⁷ The global AI software market is expected to reach \$22.6 billion by 2025, and AI applications have expanded into numerous industries, including agriculture, commerce, education, and social media.¹⁸ Understanding how AI and GAI interact with fraud schemes thus is crucial for safeguarding many industries and stakeholders. A study summarizing AI-enabled crimes highlighted six major concerns: (1) audio/video impersonation; (2) driverless vehicles as weapons; (3) tailored phishing; (4) disrupting AI-controlled systems; (5) large-scale blackmail; and (6) AI-authored fake news.¹⁹ Among them, audio/video impersonation, tailored phishing, and AI-authored fake news are fraud-related crimes that are enabled by GAI.

Humans have a strong tendency to believe in what they see and hear, but GAI-enabled impersonation technologies are challenging this inclination.²⁰ GAI has produced advanced image-editing and generation tools that generate audio, images, or videos nearly indistinguishable from real ones.²¹ When the generated audio, images, or videos contain impersonations, they are commonly referred to as “deepfakes,” a term derived from the underlying deep learning processes of GAIs.²² As early

15. *Generative AI could raise global GDP by 7%*, GOLDMAN SACHS (Apr. 5, 2023), <https://www.goldmansachs.com/insights/pages/generative-ai-could-raise-global-gdp-by-7-per-cent.html> [https://perma.cc/EHA2-DC5Z].

16. See generally Yang Bao et al., *Artificial Intelligence and Fraud Detection*, 1 INNOVATIVE TECH. AT THE INTERFACE OF FIN. AND OPERATIONS 223 (2021).

17. M. Caldwell et al., *AI-enabled future crime*, CRIME SCI. 1, 1 (2020), <https://crimesciencejournal.biomedcentral.com/counter/pdf/10.1186/s40163-020-00123-8.pdf> [https://perma.cc/H7NA-M8DX].

18. *Applications of Artificial Intelligence Across Various Industries*, FORBES (Jan. 6, 2023, 1:33 PM), <https://www.forbes.com/sites/qai/2023/01/06/applications-of-artificial-intelligence/> [https://perma.cc/Q6KC-4RT2].

19. Caldwell et al., *supra* note 17, at 1.

20. *Id.* at 6.

21. Jinjin Gu et al., *AI-enabled image fraud in scientific publications*, 3 PATTERNS 1, 1 (2022).

22. MD Shohel Rana et al., *Deepfake Detection: A Systematic Literature Review*, 10 IEEE 25494, 25494 (2022), <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9721302> [https://perma.cc/EHE6-EYUH]. The GAI technology used to create deepfakes is a combination

as 2018, a deepfake video that showed a realistic impersonation of former President Obama speaking directly to the viewer went viral.²³ Actor-director Jordan Peele, who impersonated President Obama's voice, created the video to illustrate the dangers of deepfake audio and video content depicting people saying or doing things they never actually said or did.²⁴ Currently, audio/video impersonation ranks as the most concerning type of AI-enabled crime due to its difficulty to defeat and high potential for profit.²⁵

Social engineering is the act of manipulating humans to gain access to certain confidential information,²⁶ and phishing is a social engineering attack rapidly rising in prominence. Phishing can be defined as a scalable act of deception whereby impersonation is used to obtain information from a target.²⁷ There are five stages of phishing: (1) collecting targets; (2) collecting information about the targets; (3) creating emails; (4) sending emails; and (5) finally validating and improving the emails.²⁸ Because GAI tools can generate human-like text and interact like humans, they can be used in every stage of phishing. There are two types of phishing: spear phishing and traditional phishing.²⁹ Spear phishing attacks are personalized while traditional phishing attacks are general and mass-scale.³⁰ Consequently, spear phishing attacks are expensive but effective, while traditional phishing attacks are less effective but less

of two neural networks called a Generative Adversarial Network (GAN). A GAN is a deep learning architecture that trains the two neural networks, a generative network and a discriminative network, to compete in generating authentic new data from a training dataset. The generative network uses an encoder and decoder to take an input data sample and modify it as much as possible. The discriminative network tries to predict whether the data generated by the generative network belongs in the original dataset. In other words, the two neural networks are adversarial because the generative network creates fake data while the discriminative network tries to predict whether the fake data is fake or real. As a result, the generative network generates improved versions of fake data until the discriminative network can no longer distinguish fake data from the original. *Id.*; *What is a GAN?*, AWS, <https://aws.amazon.com/what-is/gan/> [<https://perma.cc/AFG4-32PZ>].

23. Bloomberg, *How Faking Videos Became Easy — And Why That's So Scary*, FORTUNE (Sept. 11, 2018, 1:22 PM), <https://fortune.com/2018/09/11/deep-fakes-obama-video/> [<https://perma.cc/ZB4E-GKNE>].

24. *Id.*

25. Caldwell et al., *supra* note 17, at 1.

26. Amy Hetro Washo, *An interdisciplinary view of social engineering: A call to action for research*, 4 COMPUTS. IN HUM. BEHAV. REPS. 1, 1 (2021).

27. Elmer EH Lastdrager, *Achieving a consensual definition of phishing based on a systematic review of the literature*, 3 CRIME SCI. 1, 1 (2014).

28. Fredrik Heiding et al., *AI Will Increase the Quantity — and Quality — of Phishing Scams*, HARV. BUS. REV. (May 30, 2024), <https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams> [<https://perma.cc/ZU4S-UVPF>].

29. *Id.*

30. *Id.*

expensive.³¹ Currently, most phishing attacks are relatively indiscriminate, using generic messages that can be expected to be of interest to some fraction of users purely by chance.³² The attackers then rely on the ease of sending huge numbers of digital messages for a profitable gain. GAI enhances phishing by making messages appear more genuine and believable, thus increasing the response rate.³³ GAI methods also employ active learning to optimize phishing strategies and automate spear phishing, making it more cost-effective.³⁴ As a result, GAI-enabled phishing has proved to be successful. One study shows that about 60% of participants fell victim to AI-automated phishing, which is comparable to the success rates of non-AI phishing messages created by human experts.³⁵ Moreover, the entire phishing process can be automated using language learning models (LLMs), reducing the cost of phishing attacks by more than 95%.³⁶ In the last few years, AI has made phishing tactics more efficient and convincing, allowing scammers to rake in over \$12.5 billion in 2023 alone.³⁷

Finally, fake news creates fake, yet seemingly authentic, information that appears to be from a trusted source.³⁸ GAI could generate many versions of a particular content from multiple sources to boost its visibility, credibility, and impact.³⁹ Other less concerning GAI-enabled frauds include snake oil (sale of fraudulent services under the guise of AI), data poisoning (manipulation of machine learning training data to deliberately introduce specific biases), tricking face recognition (attacks on face recognition systems), and forgery (generation of fake content sold under false pretenses as to its authorship).⁴⁰

31. *Id.*

32. See Maria Vergelis et al., *Spam and Phishing in 2018*, SECURELIST (Mar. 12, 2019), <https://securelist.com/spam-and-phishing-in-2018/89701/> [<https://perma.cc/7CT4-PKU5>].

33. Caldwell et al., *supra* note 17, at 8.

34. *Id.*

35. Heiding et al., *supra* note 28.

36. *Id.*

37. Rebecca Holland, *Cybercrime cost Americans \$12.5 billion in 2023 — how to avoid becoming another scam statistic*, MONEYWISE (Feb. 21, 2025), <https://moneywise.com/life/cybercrime-cost-americans-125-billion-in-2023-how-to-avoid-becoming-another-scam-statistic> [<https://perma.cc/ZD4N-4J98>] (discussing how AI's evolution has made phishing scams and other cybercrimes more effective, and easier for criminals to use).

38. Caldwell et al., *supra* note 17, at 8.

39. *Id.*

40. *Id.* at 9-11.

II. GAI-ENABLED FRAUD SCHEMES IN MODERN REAL ESTATE MARKET

A. How GAI Can Be Used to Further Real Estate Fraud Schemes

Purchasing property should be an exciting experience, but real estate fraud tarnishes it. From the previous section, we see that GAI-enabled fraud and crimes are increasing and are potentially dangerous to society and many industries. The real estate industry is no exception to being the victim of GAI-enabled fraud. CertifID's *2024 State of Wire Fraud Report* showed that real estate is a leading target for fraud.⁴¹ In 2024, nearly 1 in 4 Americans were targeted with suspicious communications during their closing process, while approximately 1 in 10 became targets of fraud, and more than 1 in 20 became victims.⁴²

To understand how real estate fraud is committed and how AI and GAI can be used during the process, we must first understand how real estate transactions are made. Generally, there are two major types of real estate transactions: commercial real estate (CRE) and residential real estate (RRE).⁴³ In short, CRE transactions involve the buying, selling, or leasing of properties used for business purposes, while RRE transactions mainly focus on private occupancy for residential purposes.⁴⁴ A CRE deal usually involves the following phases: (1) identification and origination; (2) underwriting; (3) due diligence; and (4) closing.⁴⁵ To manage risks, parties involved in the transaction will arrange a third party as an escrow agent to hold funds or assets.⁴⁶ Sellers are usually paid in full by escrow agents on the closing date.⁴⁷ An RRE deal is simpler but also follows a similar procedure. Normally, during a real estate closing, the seller signs a warranty deed, which transfers ownership of the property from the seller

41. *2024 State of Wire Fraud Report*, CERTIFID, <https://www.certifid.com/state-of-wire-fraud> [https://perma.cc/5KYW-SP3X].

42. *Id.*

43. *Commercial v. Residential Real Estate What's The Difference? What Does a Commercial Real Estate Lawyer Do?*, THE ORLANDO L. GRP., PL (Feb. 1, 2023), <https://www.theorlandolawgroup.com/blog/all/commercial-v-residential-real-estate/> [https://perma.cc/898L-DFTJ] [hereinafter *Commercial v. Residential Real Estate*].

44. *Id.*

45. *Overview of the Commercial Real Estate Transaction Lifecycle*, FIRST NAT'L REALTY PARTNERS (Feb. 12, 2021), https://fnrpusa.com/blog/overview-of-the-commercial-real-estate-transaction-lifecycle/?utm_term=blog%2Boverview-of-the-commercial-real-estate-transaction-lifecycle [https://perma.cc/5KS3-DVCG].

46. *Commercial v. Residential Real Estate*, *supra* note 43.

47. Jennifer Ferri, *Understanding the Role of Escrow in a Real Estate Transaction*, TITLE JUNCTION (Oct. 24, 2024), <https://title-junction.com/2024/10/24/escrow-in-a-real-estate-transaction/> [https://perma.cc/XP2V-A5CV].

to the buyer.⁴⁸ The deed then gets recorded, making the transaction official.⁴⁹

With the rapid development of digitalization and the increasing use of GAI, a potential buyer may face fraudulent property listings,⁵⁰ imposter scams, and deed fraud.⁵¹ A 2023 study found that 41% of recent buyers took the first step in the buying process by looking online at properties for sale, while only 21% of buyers first contacted a real estate agent.⁵² It is reported that a \$1.6 million house that appeared on Zillow in Kansas City recently listed for \$10,200 turned out to be a scam listing.⁵³ The fake seller required all interested buyers to send a nonrefundable amount of \$200 for a walk-through at a house that was not for sale.⁵⁴ Some scammers also target vacant land and properties that have no mortgages or other liens.⁵⁵ They will pose as the actual landowner, asking a real estate agent to list the property.⁵⁶ To make it more convincing, they will present fraudulent deeds to make the deal go through.⁵⁷

How do fraudsters obtain fraudulent deeds? In Florida, for a deed to be recorded properly, it must have the signed names of the persons conveying and receiving property, the two witnesses, and the notary

48. *What Documents Are Needed for a Real Estate Closing in Florida*, ST PETERSBURG REAL EST. ATT'Y BATTAGLIA, ROSS, DICUS & MCQUAID, P.A. (Mar. 4, 2023), <https://www.727realestatelaw.com/what-documents-are-needed-for-a-real-estate-closing-in-florida/> [<https://perma.cc/FVF7-BG9A>] (reviewing key documents for real estate closings in Florida).

49. *What You Need to Know About a Deed in a Real Estate Transaction*, FED. STANDARD ABSTRACT (July 17, 2023), <https://www.federalstandardabstract.com/what-you-need-to-know-about-a-deed-in-a-real-estate-transaction/> [<https://perma.cc/UM9C-SGFB>].

50. *Protecting Your Most Valuable Asset, Your Real Estate*, GOMEZ L., <https://gomezlawla.com/blog/navigating-the-intersection-of-ai-and-real-estate-insights-risks-and-legal-implications/> [<https://perma.cc/U7TP-YGHM>] (“Be vigilant of scams involving AI-generated images and descriptions for non-existent properties.”).

51. Aleysha Velez Vazquez, *AI Fraud Threatens Mortgage Security*, SIMPLY TITLE (Mar. 7, 2025), <https://www.simply-title.com/post/ai-fraud-threatens-mortgage-security> [<https://perma.cc/GVS5-Q8F2>].

52. *Highlights From the Profile of Home Buyers and Sellers*, NAT'L ASS'N OF REALTORS, <https://www.nar.realtor/research-and-statistics/research-reports/highlights-from-the-profile-of-home-buyers-and-sellers> [<https://perma.cc/FT3R-L873>].

53. Joseph Hernandez, *Scam listed KC home for sale & charged \$200 for tours. What to know about fake listings*, THE KAN. CITY STAR (July 11, 2024, 12:55 PM), <https://www.kansascity.com/kc-city-guides/tips/article289176969.html> [<https://perma.cc/Z8A3-6VB3>].

54. *Id.*

55. Melissa Dittmann Tracey, *Scammers Are Plotting to Sell Vacant Land Fraudulently*, NAT'L ASS'N OF REALTORS (Oct. 23, 2023), <https://www.nar.realtor/magazine/real-estate-news/law-and-ethics/scammers-are-plotting-to-sell-vacant-land-fraudulently> [<https://perma.cc/7RR9-EEY7>].

56. *Id.*

57. *Id.*

public or other officers authorized to take acknowledgments.⁵⁸ Fraudsters use property register databases to look for target properties and then use property records as templates to forge deeds and find a phony notary service to complete the transfer.⁵⁹ They usually target vulnerable property that meets most of the following criteria: (1) vacant; (2) located in a blighted area; (3) not maintained by property owner; (4) delinquent on taxes; (5) unencumbered by liens; or (6) whose owner does not live nearby.⁶⁰ Once they have the deeds recorded in front of the county clerk, they become the “rightful” owner of the property and sell it to one or more good-faith buyers for money or use it as collateral on a loan.⁶¹

This is a growing problem in many states, especially Florida.⁶² In fact, more than 54% of real estate professionals experienced deed fraud firsthand in the second half of 2023.⁶³ In March 2024, a community organizer in Detroit, Michigan, named Zina Thomas was charged with stealing more than thirty homes in and around the city by forging quitclaim deeds transferring the properties to fictitious entities, and then selling them to unwitting third parties.⁶⁴ The harm of this type of fraud is certainly destructive because, for most Americans, a home is their most valuable asset, and having it stolen and transferred to third parties can be a devastating event. The rightful homeowner will end up hiring an attorney to keep the innocent thirty-party buyer off his property, which can be time-consuming and costly.

Fraudsters may even find a way to trick buyers into a legitimate deal by impersonating the true seller or the escrow agent.⁶⁵ In February 2024,

58. FLA. STAT. § 695.26 (2024).

59. Ryan Toohil, *How Can Someone Steal Your House Deed?*, IDENTITY GUARD (Oct. 16, 2023), <https://www.identityguard.com/news/how-can-someone-steal-your-house-deed> [https://perma.cc/PUX8-NLKW].

60. Jennifer Coddling, *Florida - Leading The Fight In Preventing Deed Fraud*, ALEXANDER S. BUCHANAN, PLLC (Oct. 24, 2023), <https://www.attorneybuchanan.com/florida-leading-the-fight-in-preventing-deed-fraud> [https://perma.cc/YV2N-X8YC].

61. Larry Silverstri, *Florida property title fraud is a problem. Here's a way to protect yourself*, TAMPA BAY TIMES (Feb. 22, 2024), <https://www.tampabay.com/opinion/2024/02/22/florida-property-title-fraud-is-problem-heres-way-protect-yourself/> [https://perma.cc/7HMM-JNRP].

62. *Property deed fraud growing problem in Florida; state offers assistance in detection*, FOX 13 TAMPA BAY (Mar. 1, 2024, 8:49 AM), <https://www.fox13news.com/news/property-deed-fraud-growing-problem-in-florida-state-offers-assistance-in-detection> [https://perma.cc/JR9B-KLLN].

63. *Id.*

64. Keith Griffith, *Deed fraud is on the rise — here's how to protect your home*, N.Y. POST (Apr. 1, 2024), <https://nypost.com/2024/04/01/real-estate/deed-fraud-is-on-the-rise-heres-how-to-protect-your-home/> [https://perma.cc/F5QZ-ZTRQ].

65. Danica De Vera, *The 10 Most Common Scams in Business Sales*, CONSULTANTS, LLC (Mar. 1, 2024, 10:42 AM), <https://cfoconsultants.net/the-10-most-common-scams-in-business-sales/> [https://perma.cc/QDW5-YACA] (“In this scam, fraudsters impersonate escrow services to deceive sellers into transferring their business assets or sensitive information.”).

a British multinational design and engineering company in Hong Kong fell victim to a deepfake scam, suffering a loss of \$25 million to fraudsters.⁶⁶ According to Hong Kong police, the employee, a finance worker, was duped into attending a video call with people he believed were the chief financial officer and other staff members, all of whom turned out to be deepfake recreations.⁶⁷ The scam first started with a phishing email allegedly from the company's U.K. office, specifying a need for a secret transaction to be carried out.⁶⁸ The employee was suspicious at first, but his doubts were put aside after he had a video with the CFO and several other corporate executives he recognized.⁶⁹ However, a week later when he checked with the company's home office to ask about the status of the secret deal, he realized that there was no secret deal at all and that he was scammed.⁷⁰

As of today, the Author has not found reporting of fraudsters using deepfake videos in a real estate transaction to scam buyers.⁷¹ Nevertheless, fraudsters conduct impersonation through other, easier means such as phishing emails.⁷² It is reported that a couple purchasing a house received a legitimate email from the title company before closing on their home purchase.⁷³ The email alerted them that they would receive wiring instructions the next day, and when they received the email with an identical email signature and wiring instructions the next day, they moved forward and sent the payment.⁷⁴ However, it turned out that the second email was sent by a fraudster impersonating the contact at the title company.⁷⁵

The application of GAI will increase both the likelihood of these scams and their success rates to a new level. First of all, fraudsters can apply GAI to trick buyers into illegitimate deals.⁷⁶ They can successfully target more vacant land or other not-for-sale properties to create fake property listings on a large scale using GAI.⁷⁷ They can make images of

66. Kathleen Magramo, *British engineering giant Arup revealed as \$25 million deepfake scam victim*, CNN BUS. (May 17, 2024), <https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html> [https://perma.cc/X3FZ-EB5U].

67. *Id.*

68. *Id.*

69. *Id.*

70. *Id.*

71. *See id.*

72. *See infra* note 73.

73. Breck Dumas, *Real estate fraud risk is on the rise, and victims are sounding the alarm*, FOX BUS. (Feb. 6, 2024, 8:00 AM), <https://www.foxbusiness.com/lifestyle/real-estate-fraud-risk-on-rise-victims-sounding-alarm> [https://perma.cc/2TNV-7LFL].

74. *Id.*

75. *Id.*

76. *See id.*

77. *AI-Driven Fraud: The Hidden Threat in Real Estate*, FIRST AM. (Feb. 20, 2025),

the properties look deceptively better to attract more potential buyers. They can also use deepfake technologies to create fake images, videos, or voices of persons such as real estate agents or sellers to trick buyers into believing that the deal is legitimate.⁷⁸ Deepfakes can also be used to create false identification documents in creating a fraudulent deed.⁷⁹ Second, fraudsters may use GAI to impersonate important parties in a legitimate deal.⁸⁰ Fraudsters may utilize GAI to create specific and tailored phishing emails to trick buyers into making payments to them or downloading malware that steals their personal and financial information.⁸¹ They can also use deepfakes to impersonate sellers, escrow agents, or even lawyers in a virtual meeting to harvest the funds through fraud.⁸²

Increasing digitalization makes GAI-enabled real estate frauds a more pressing issue. According to the National Association of Realtors, 96% of realtors use a smartphone with wireless email and internet capabilities daily.⁸³ Zoom had 10 million daily meeting participants in December of 2019, but now it averages 300 million daily active users in meetings.⁸⁴ In the meantime, more and more people are working remotely.⁸⁵ As of 2023, 12.7% of full-time employees work from home, while 28.2% work a hybrid model.⁸⁶ It is expected that 32.6 million Americans will work

<https://www.firstam.com/home-buying-guide/ai-driven-fraud-the-hidden-threat-in-real-estate/#:~:text=AI%2Dpowered%20fraud%20in%20real%20estate%20is%20growing%2C%20with%20scammers,staying%20informed%20about%20AI%20scams> [https://perma.cc/GLJ4-L4S3] (“Properties without an owner-occupant, such as a vacant lot, a second home, or a rental property, are common targets for scammers since it's less likely the owner will discover the fraud.”).

78. *Id.*

79. *Id.* (“AI tools also make it easier to quickly fabricate correspondence, identification, deeds, mortgages, video, and voices, which can be indistinguishable from a real document or person.”).

80. *Id.* (“In real estate transactions, scammers can use deepfake audio or video to impersonate real estate agents or other professionals involved in the transaction, leading to fraudulent communications that provide false information or instructions.”).

81. Sharon Shea, *How is AI making phishing attacks more dangerous*, TECHTARGET (Oct. 22, 2024), <https://www.techtargget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous> [https://perma.cc/P9G5-S3BF].

82. *AI-Driven Fraud: The Hidden Threat in Real Estate*, *supra* note 77.

83. *Real Estate in a Digital Age*, NAT'L ASS'N OF REALTORS, <https://www.nar.realtor/research-and-statistics/research-reports/real-estate-in-a-digital-age> [https://perma.cc/4SDN-6ZRK] (last visited Mar. 11, 2024).

84. Matthew Woodward, *Zoom User Statistics: How Many People Use Zoom in 2025?*, SEARCH LOGISTICS (June 23, 2023), <https://www.searchlogistics.com/learn/statistics/zoom-user-statistics/> [https://perma.cc/4XX3-3LM6].

85. *The Future of Work: Remote Work Trends and Business Continuity*, PREPARIS (Jan. 30, 2024), <https://www.preparis.com/article/future-work-remote-work-trends-and-business-continuity> [https://perma.cc/TVB6-4TKB].

86. *Id.*

remotely by 2025.⁸⁷ Therefore, it can be expected that fraudsters will have more scenes to commit their scams. For example, they may impersonate an attorney's voice using GAI and call the buyer using a number spoofing software to make the call appear as though it was from the actual attorney to trick the buyer into making the payment to the fraudster's account or hold a Zoom meeting with the buyer acting as their attorney or agent.

B. Real Estate Fraud in the Growing Florida Market

In recent years, Florida has experienced rapid population growth,⁸⁸ which has contributed to the increasing demand for housing, consequently driving the Florida residential real estate market growth.⁸⁹ The Sunshine State shines equally bright in the commercial real estate industry.⁹⁰ In 2024, the Florida real estate market remains a focal point of attention for investors, homeowners, and economists.⁹¹ As of March 2024, Florida's median home price increased by 3.7% from the previous year, reaching \$415,300.⁹² Because of its growing and lucrative real estate market, Florida has become a target for fraudsters who specialize in real estate fraud.⁹³ About 54% of real estate professionals in Florida have experienced property deed fraud firsthand in just the second half of 2023.⁹⁴ Many fraudsters commit deed and title scams by stealing a person's identity; therefore, it is no surprise that Florida ranked second in a Federal Trade Commission (FTC) identity theft report that analyzed identity theft rates for every state in the U.S.⁹⁵ Because of its growing real estate marketing and increasing fraud incidents, Florida has become a pioneer in promulgating programs and laws regarding real estate fraud prevention.

87. Katherine Haan, *Top Remote Work Statistics and Trends*, FORBES (last updated June 12, 2023, 5:29 AM), <https://www.forbes.com/advisor/business/remote-work-statistics/> [https://perma.cc/32GH-LM89].

88. Marc Perry et al., *New Florida Estimates Show Nation's Third-Largest State Reaching Historic Milestone*, U.S. CENSUS BUREAU (Dec. 22, 2022), <https://www.census.gov/library/stories/2022/12/florida-fastest-growing-state.html> [https://perma.cc/893D-TSLN].

89. Ed DiMarco, *Florida Real Estate Market in 2024: Overview & Predictions*, NAPLES.ED.COM (May 5, 2024), <https://www.naplesed.com/post/florida-real-estate-market-in-2024> [https://perma.cc/TDY4-YYTJ].

90. *Id.*

91. *Id.*

92. *Id.*

93. Griffith, *supra* note 64.

94. *Id.*

95. Jennifer Streaks, *States with the Most and Least Identity Theft*, BUS. INSIDER (July 31, 2024, 10:10 AM), <https://www.businessinsider.com/personal-finance/credit-score/identity-theft-by-state> [https://perma.cc/6LNJ-ZMQ4].

III. GAI-ENABLED FRAUD PREVENTION, REGULATIONS, AND POLICY SUGGESTIONS

A. *GAI-Enabled Real Estate Fraud Prevention*

In real estate fraud, GAI is a double-edged sword. It can either be used by fraudsters to commit real estate fraud or used by real estate professionals and government officers to detect and prevent real estate fraud.⁹⁶ By leveraging GAI-powered transaction monitoring and identity verification systems, real estate professionals can identify and prevent suspicious activities early on.⁹⁷

First, GAI technologies can be applied in four ways to detect phishing attacks: (1) deep learning; (2) machine learning; (3) hybrid learning; and (4) scenario-based techniques or phishing attack detection.⁹⁸ Deep learning methods can learn to detect phishing attacks by processing batches of input data and assigning weights to the data to distinguish phishing attacks from legitimate traffic.⁹⁹ To train a machine learning model for a learning-based detection system, the data at hand must have features that are related to phishing and legitimate website classes.¹⁰⁰ Different classifiers are used to detect a phishing attack.¹⁰¹ Deep learning algorithms, particularly convolutional neural networks (CNNs), long short-term memory (LSTM), and gated recurrent unit (GRU) models, have shown promising potential on different classification tasks.¹⁰² Scenario-based detections are only applicable to a particular environment, and a hybrid learning approach has relatively inconsistent accuracy rates.¹⁰³ Therefore, deep learning and machine learning algorithms are great tools for detecting phishing emails and, consequently, preventing real estate fraud. Moreover, these algorithms can analyze transaction patterns, thus helping professionals identify other fraudulent activities in real estate transactions.¹⁰⁴ For example, some researchers have proposed that clustering analysis can help distinguish fake real estate listings from real ones based on datasets curated by industry experts.¹⁰⁵

96. Abdul Basit et al., *A comprehensive survey of AI-enabled phishing attacks detection techniques*, 76 TELECOMM. SYS. 139, 139 (2021).

97. *See id.*

98. *Id.* at 141.

99. *Id.* at 143.

100. *Id.* at 144.

101. Basit et al., *supra* note 96, at 144.

102. *Id.* at 143.

103. *Id.* at 149.

104. Maifuza Mohd Amin et al., *Clustering analysis for classifying fake real estate listings*, PEERJ COMPUT. SCI. June 2024, at 1, 2.

105. *Id.* at 1.

Second, researchers have put forward new approaches to recognize deepfake content to prevent the misuse of deepfakes. Since the influx of deep learning software that allows any user to create fabricated content, many initiatives have been proposed to create anti-deepfake tools. The United States Defense Advanced Research Projects Agency promoted the Media Forensics program¹⁰⁶ to encourage the development of anti-deepfake methodologies, and Facebook started the Deepfake Detection Challenge to advance anti-deepfake technologies.¹⁰⁷ Christopher Chun Ki Chan proposed a deep learning algorithm that combined multiple LSTMs with a CNN to track and trace digital content as a first step to combat deepfakes.¹⁰⁸ Yang suggested a new visual speaker authentication scheme based on a deep convolutional neural network to combat deepfakes.¹⁰⁹ Experiments have demonstrated that the Yang approach can achieve an accurate authentication result against human imposters.¹¹⁰ Jayashre and Amsaprabhaa have proposed a hybrid-optimized, deep feature, fusion-based deepfake detection that utilizes a spotted hyena optimizer to detect deepfake videos.¹¹¹ The Jayashre and Amsaprabhaa framework successfully detected deepfake videos with an accuracy exceeding 90% on subsets like DeepFakes, FaceSwap, and Face2Face.¹¹²

Although researchers are working on new technologies to combat deepfakes, new threats may materialize before effective solutions are created to prevent deepfake-assisted fraud. There are many highly sophisticated and difficult-to-distinguish deepfakes that are being used for criminal purposes, affecting a wide range of industries including real estate. Therefore, the regulation of GAI-enabled technologies is imminent.

B. Current Real Estate Fraud Prevention Programs and Statutes

Most states have statutes addressing fraud and theft. For example, in Florida, any person engaged in a scheme to defraud and obtain property

106. *MediFor: Media Forensics*, DARPA, <https://www.darpa.mil/program/media-forensics> [https://perma.cc/AY6Q-HJ3J].

107. Eliza Strickland, *Facebook AI Launches Its Deepfake Detection Challenge*, IEEE SPECTRUM (Dec. 11, 2019), <https://spectrum.ieee.org/facebook-ai-launches-its-deepfake-detection-challenge> [https://perma.cc/4KDS-H8ST].

108. Christopher Chun Ki Chan et al., *Combating deepfakes: Multi-LSTM and blockchain as Proof of Authenticity for Digital Media*, 2020 IEEE/ITU INT'L CONF. ON A.I. FOR GOOD (AI4G) 2020, at 55, 55.

109. Chen-Zhao Yang et al., *Preventing DeepFake Attacks on Speaker Authentication by Dynamic Lip Movement Analysis*, 16 IEEE TRANSACTIONS ON INFO. FORENSICS AND SEC. 1841, 1841 (2021).

110. *Id.*

111. Jayashre K. & Amsaprabhaa M., *Safeguarding media integrity: A hybrid optimized deep feature fusion based deepfake detection in videos*, 142 COMPUT. & SEC. 1, 1 (2024).

112. *Id.*

with an aggregate value of \$50,000 or more is guilty of a felony of the first degree.¹¹³ Similarly, under Virginia Code § 18.2-186, it is a Class 1 misdemeanor to make fraudulent misrepresentations to obtain property.¹¹⁴ Due to increasing real estate fraud, some states have adopted targeted legislation to prevent it from happening. For example, in 2023, the Florida legislature enacted § 28.2225 of the Florida Statutes, establishing an identity verification pilot program to prevent title fraud.¹¹⁵ The new law requires anyone who records a deed to present a government-issued photo ID before the deed is processed.¹¹⁶ The requirement for photo ID makes it easier for law enforcement to verify the identity of the parties engaged in property-related transactions and investigate fraudulent activity more thoroughly.¹¹⁷ Moreover, it also requires the address of each witness to a real estate conveyance be included on any real property conveyance.¹¹⁸ Similarly, in 2024, Georgia passed House Bill 1292, which requires clerks of the superior courts to obtain photographic identification cards of individuals who present deeds or other instruments for recording.¹¹⁹ These laws add another layer of protection against fraudsters by verifying the identities of the parties engaged in property-related transactions before final conveyance.

Other than legislation, many states have encouraged their citizens to opt into a free property fraud alert system where a property owner will receive an email or phone notification regarding transactions of their property.¹²⁰ The sign-up procedure usually requires a simple entry of an email address and some type of property identification information (such as individual name, business name, or parcel number) for a property owner to receive an alert.¹²¹ Even though these fraud alert systems are fully voluntary and do not prevent fraud from happening, they provide early warnings for property owners to take appropriate actions before the fraud develops further.

113. FLA. STAT. § 817.034(4) (2023).

114. VA. CODE ANN. § 18.2-186(A) (2020).

115. FLA. STAT. § 28.2225 (2023).

116. *Id.*

117. *Pilot Program's Goal is to Stem Property Fraud*, THE FLA. BAR (June 30, 2023), <https://www.floridabar.org/the-florida-bar-news/pilot-programs-goal-is-to-stem-property-fraud/> [https://perma.cc/FJA9-L6F4].

118. *See id.*

119. H.B. 1292, 2023-2024 Leg., Reg. Sess. (Ga. 2024).

120. *See, e.g.*, Recording Notification Services, ALACHUA CNTY. CLERK OF THE CT., <https://isol.alachuaclerk.org/RecordingNotificationWebLive/Subscribe> [https://perma.cc/2VZ7-FKHM].

121. *Id.*

C. U.S. Regulations Regarding GAI Use in Fraud

Currently, there are no known regulations specifically addressing GAI-enabled real estate fraud. In general, AI-related regulations in the United States are relatively scarce.¹²² The world's first and currently most comprehensive law is the EU AI Act.¹²³ Proposed by the European Commission in April 2021, the EU AI Act categorizes AI systems into various risk levels and regulates them accordingly.¹²⁴ Even though the United States has not adopted a comprehensive AI law so far, it has noticed the threats brought by certain GAI technologies like deepfakes. There is no federal regulation specifically overseeing deepfake technologies, but a patchwork of federal and state laws governs their use. On December 20, 2019, President Trump signed the Deepfake Report Act of 2019, the nation's first federal law related to deepfakes.¹²⁵ The law directs the Department of Homeland Security to issue annual reports on deepfake technology.¹²⁶ In the same year, Virginia and Texas enacted laws criminalizing certain deepfakes.¹²⁷ Virginia became the first state in the nation to impose criminal penalties on the distribution of nonconsensual deepfake pornography, while Texas became the first state in the nation to prohibit the creation and distribution of deepfake videos that intend to harm candidates for public office or influence elections.¹²⁸

On September 21, 2023, Congresswoman Yvette D. Clarke (D-NY) and Congressman Glenn Ivey (D-MD) introduced the DEEPFAKES Accountability Act of 2023 to require creators to digitally watermark deepfake content.¹²⁹ Similarly, the Protecting Americans from Deceptive AI Act introduced March of 2024 requires the National Institute of Standards and Technology to work on setting standards and guidelines relating to the identification of AI-generated content.¹³⁰ Around the same time, the Senate introduced the NO FAKES Act of 2024, which creates

122. Yoon Chae, *US AI Regulation Guide: Legislative Overview and Practical Considerations*, 3 J. ROBOTICS, A.I. & L. 17, 17 (2020).

123. Yoshija Walter, *Managing the Race to the Moon: Global Policy and Governance in Artificial Intelligence Regulation—A Contemporary Overview and an Analysis of Socioeconomic Consequences*, 4 DISCOVER A.I. at 1, 4 (2024).

124. *Id.*

125. Jason C. Chipman & Stephen W. Preston, *First Federal Legislation on Deepfakes Signed Into Law*, WILMERHALE (Dec. 23, 2019), <https://www.wilmerhale.com/insights/client-alerts/20191223-first-federal-legislation-on-deepfakes-signed-into-law> [<https://perma.cc/RQ3N-H7XT>].

126. *Id.*

127. *Id.*

128. *Id.*

129. DEEPFAKES Accountability Act, H.R. 5586, 118th Congress (2023-2024).

130. Protecting Consumers from Deceptive AI Act, H.R. 7766, 118th Congress (2023-2024).

new federal intellectual property rights over a person's digital replica that can be enforced through a civil action.¹³¹

In the 2024 legislative session, at least forty-five states, Puerto Rico, the Virgin Islands, and Washington, D.C., introduced AI bills, and thirty-one states, Puerto Rico and the Virgin Islands adopted resolutions or enacted legislation.¹³² On April 26, 2024, Florida's Governor signed into law an act relating to artificial intelligence use in political advertising.¹³³ The act provides that a political advertisement must state a disclaimer if it contains digital content created with GAI, depicting something that did not happen, and created with the intent to injure a candidate or to deceive.¹³⁴ Although this disclaimer is not required in other AI-generated content, it is a sign that legislatures have noticed the harm of AI-automated content.¹³⁵ Similarly, Oklahoma House Bill 3453, if passed, would require a watermark on AI-generated content to verify the authenticity of a creative product and to approve derivative media generated by AI that uses a person's audio recordings or images.¹³⁶ Ohio also has similar watermark requirements, and Utah requires disclosure of AI use.¹³⁷

The executive branch also promulgated rules to combat AI-enabled fraud.¹³⁸ In 2019, President Trump issued the executive order Maintaining American Leadership in Artificial Intelligence, aiming to enhance United States capabilities in AI.¹³⁹ It also directly impacts the regulation of AI in the U.S., as the Office of Management and Budget and the National Institute of Standards and Technology were ordered to establish standards to enable the regulation of AI.¹⁴⁰ On October 30, 2023, President Biden issued the landmark executive order Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence to

131. NO FAKES Act of 2024, S. 4875, 118th Congress (2023-2024).

132. *Artificial Intelligence 2024 Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Sept. 9, 2024), <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation> [<https://perma.cc/FBX3-5PSV>].

133. FLA. STAT. § 106.145 (2024).

134. *Id.* The disclaimer must be stated prominently and read: "Created in whole or in part with the use of generative artificial intelligence (AI)."

135. *Id.*

136. Owen Davis & David Stauss, *A look at proposed US state private sector AI legislation*, IAPP (Feb. 28, 2024), <https://iapp.org/news/a/a-look-at-proposed-u-s-state-private-sector-ai-legislation> [<https://perma.cc/FAB8-JZRU>].

137. *Artificial Intelligence 2024 Legislation*, *supra* note 132.

138. See John Frank Weaver, *Everything is not the Terminator: What Does the Executive Order Calling for Artificial Intelligence Standards Mean for AI Regulation?*, 2 J. ROBOTICS, A.I. & L. 373, 373 (2019).

139. *Id.*

140. *Id.*

establish new standards for AI safety and security.¹⁴¹ One of the goals of the 2023 Executive Order is to protect Americans from AI-enabled fraud and deception by establishing standards and best practices for detecting AI-generated content and authenticating official content.¹⁴² To achieve this goal, the Department of Commerce will develop guidance for content authentication and watermarking to clearly label AI-generated content.¹⁴³ Considering surging complaints around impersonation fraud, another executive department, the FTC, has proposed rules prohibiting AI impersonation of individuals, government, and businesses.¹⁴⁴ The proposed rules would enable the FTC to directly seek monetary relief in federal court from scammers that use government seals or business logos, spoof government and business emails and web addresses, and falsely imply government or business affiliation.¹⁴⁵

D. Discussion

For bad actors, the profits of using GAI technologies such as deepfakes to commit real estate frauds are extremely high. Even though many states have realized the potential threat of GAI-enabled real estate frauds, there is limited legal protection. Many states rely on voluntary fraud alert systems, general identify theft, and impersonation laws to punish fraudsters. Why would there be inadequate legal regulations concerning GAI and fraud? Some believe that the U.S. government purposefully delays the adoption of comprehensive AI laws to keep the AI industry growing.¹⁴⁶ Since the United States could potentially get into a head-to-head competition with China, the second-largest leader in the AI race, the United States is motivated not to put on too many regulatory blocks too fast.¹⁴⁷

Another reason why laws lag behind technological development is the relatively slow pace at which laws are adopted.¹⁴⁸ The pacing problem

141. *WHAT THEY ARE SAYING: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, THE WHITE HOUSE (Oct. 30, 2023), <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/10/31/what-they-are-saying-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/> [https://perma.cc/UP58-ZDLT].

142. *Id.*

143. *Id.*

144. *FTC Proposes New Protections to Combat AI Impersonation of Individuals*, FED. TRADE COMM’N (Feb. 15, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals> [https://perma.cc/M4TG-R8MA].

145. *Id.*

146. Walter, *supra* note 123, at 12.

147. *Id.* at 7.

148. GARY E. MARCHANT, *THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT* 1, 28 (Gary E. Marchant et al. eds., 1st ed. 2011).

faced by legal institutions has two dimensions. On the one hand, many existing legal frameworks are based on a static, rather than dynamic, view of society and technology.¹⁴⁹ On the other hand, legal institutions are slowing down with respect to their ability to adjust to changing technologies.¹⁵⁰ Issues are often not addressed based on their importance but rather on their perceived political urgency.¹⁵¹ Therefore, it often takes some type of crisis to shock the Legislature into opening this legislative window.¹⁵²

Partly because laws are harder to pass, the Executive Branch utilizes its capabilities to make regulations to combat challenges brought by AI development. Professors Ariel Bendor and Sharon Yadin point out that regulatory agencies often hold all three governmental functions, including judicial-like punitive sanctioning powers and comprehensive legislative powers for setting major regulations, with almost no supervision by other branches of government.¹⁵³ They also indicate that courts tend to grant de facto immunity from judicial review to many regulatory actions of administrative agencies under different types of deference doctrines, leading to substantial misalignment between constitutional separation of powers and regulatory mechanisms.¹⁵⁴

CONCLUSION AND SUGGESTIONS

Real estate and AI are two growing markets. Ill-intended fraudsters can use GAI-enabled technologies such as deepfake and phishing attacks to commit high-stakes real estate fraud. Many states have noticed this problem and have promoted voluntary property fraud alert programs and some regulations to combat deed fraud. For example, § 28.2225 of the Florida Statutes requires anyone who records a deed to present a government-issued photo ID before the deed is processed. There is also a growing consensus among states and the federal government to require watermarks or disclaimers on deepfake-created content.¹⁵⁵

However, there remains a huge gap between GAI development and regulation since there currently is no comprehensive AI act in the United States or an Act specifically targeting deepfakes. To prevent GAI-enabled real estate fraud, we can take advantage of other GAI technologies. For example, we can create voluntary or mandatory training modules

149. *Id.* at 23.

150. *Id.*

151. *Id.*

152. *Id.*

153. Ariel Bendor & Sharon Yadin, *Regulation and the Separation of Powers*, 28 S. CAL. INTERDISC. L.J. 357, 357 (2019).

154. *Id.*

155. Examples include the DEEPFAKES Accountability Act of 2023, Florida H.B. 919 and Oklahoma H.B. 3453.

powered by GAI to educate real estate professionals about real estate fraud schemes and fraud prevention techniques. We can also use GAI-driven virtual assistants to educate potential buyers about common fraud schemes and warning signs. The real estate industry can work with the government to create GAI-powered collaborative platforms that facilitate secure information among real estate agents, banks, and law enforcement. Technologies that can detect deepfake content or other GAI impersonation technologies should be encouraged to use in high-stakes virtual meetings. On the other hand, county clerks should verify the authenticity of government-issued photo IDs before recording the deed. The executive and legislature branches should establish incentives for individuals and professionals to report suspected fraud, invest more energy and resources into research on AI fraud prevention, and publish laws that target GAI-enabled fraud in general business transactions.

By adopting these measures, we will be in a stronger position to prevent and tackle real estate fraud effectively in the age of GAI.