Attorney General Advisory on the Application of the Commonwealth's Consumer Protection, Civil Rights, and Data Privacy Laws to Artificial Intelligence

The Office of the Attorney General ("AGO") issues this Advisory to provide guidance to developers, suppliers, and users of artificial intelligence and algorithmic decision-making systems (collectively, "AI")[1] about their respective obligations under the Massachusetts Consumer Protection Act, G.L. c. 93A, § 2, and the regulations promulgated in 940 Code Mass. Regs. 3.00 *et seq.* and 940 Code Mass. Regs. 5.00 *et seq.* Additionally, this Advisory provides guidance on the obligations of developers, suppliers, and users of AI under the Massachusetts Anti-Discrimination Law, G.L. c. 151B, § 4 and the Data Security Law, G.L. c. 93H, and implementing regulations, 201 Code Mass. Regs. 17.00, *et seq.*[2]

The Promise and Risks of Artificial Intelligence

AI has tremendous potential benefits to society. It presents exciting opportunities to boost efficiencies and cost-savings in the marketplace, foster innovation and imagination, and spur economic growth. This is particularly true in the Commonwealth: home to the nation's leading biotech and life sciences industries and world-renowned research and higher educational institutions at the forefront of this emerging technology. The AGO thus encourages innovation and the use of AI systems[3] where such usage complies with Massachusetts law. However, AI systems have already been shown to pose serious risks to consumers, including bias, lack of transparency or explainability, implications for data privacy, and more. Despite these risks, businesses and consumers are rapidly adopting and using AI systems which now impact virtually all aspects of life.

AI systems are complex, and their usage is often hidden from consumers. Moreover, because AI is used broadly throughout an ever-increasing number of contexts and industries, consumers in the Commonwealth cannot meaningfully opt out of most AI use cases. As a result, consumers

[1] There is no settled definition for AI. For purposes of this Advisory, the AGO defines "artificial intelligence" or "AI" as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action." Executive Order 14110 on the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, section 3(b), October 30, 2023, *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/. This Advisory also applies to "generative AI" which is "the class of AI models that emulate the structure and characteristics of input date in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content." *Id.,* section 3(p).

[2] This Advisory provides the Attorney General's guidance on the general application of the Commonwealth's consumer protection, civil rights, and data privacy laws to AI. This Advisory does not address all laws that may apply to AI or that may be enforced by the Attorney General in this area, nor does it address all potential AI applications or use cases.

[3] The term "AI systems" means "any data system, software, hardware, application, tool, or utility that operation in whole or in part using AI." *Supra* note 1, at section 3(e).

lack the skill, ability, and opportunity to challenge, avoid or test the appropriateness of AI as applied to them or to business transactions in which they are involved. Yet, consumers are harmed when AI does not function as intended or does not meet minimum quality and efficacy standards that would apply to other consumer goods or services.

Developers and suppliers promise that their AI systems and technology are accurate, fair, effective, and appropriate for given use cases. At the same time, developers and suppliers also claim that AI is a "black box", meaning that they do not know exactly how AI performs various processes or generates its results. They continue to market and sell AI systems knowing these shortfalls and that they may cause harm to consumers. There are many instances where AI systems fall short of suppliers' promises. AI has been found to generate false information or results that are biased or discriminatory. These deficiencies and instances of poor quality are especially concerning when AI is used for processes that impact consumers' livelihood, reputation, or economic well-being.

Additionally, AI systems are being deployed in ways that can deceive consumers and the public as in the case of chatbots used to perpetrate scams or to surreptitiously collect sensitive personal data from consumers, deepfakes[4], and voice cloning[5] used for the purpose of deceiving or misleading a listener about the speaker's true identity.

This Advisory is intended to address and ultimately mitigate these risks by clarifying for consumers, developers, suppliers, and users of AI systems that existing state laws and regulations apply to this emerging technology to the same extent as they apply to any other product or application within the meaning of the Attorney General's Consumer Protection regulations in the stream of commerce.[6]

The Laws and Regulations

Consumers in the Commonwealth enjoy the protection of Chapter 93A which creates a "flexible set of guidelines" as to what should be considered "unfair and deceptive" and which is intended "to grow and change with the times." *Nei v. Burley,* 388 Mass. 307, 313 (1983). The novelty, complexity and claimed inscrutability of AI systems do not take their marketing, sale and use beyond the reach of Chapter 93A. Rather, considering the concerns about AI systems referenced

[4] A "deepfake" "is an image, or a video or audio recording, that has been edited using an algorithm to replace the person in the original with someone else (especially a public figure) in a way that makes it look authentic. The fake in deepfake is transparent: deepfakes are not real." Merriam-Webster, https://www.merriam-webster.com/dictionary/deepfake.

[5] "Voice cloning" "builds a digital copy of a person's unique voice, including speech patterns, accents, voice inflection and even breathing, by training an algorithm with a sample of a person's speech. Mohamed Lazzouni, "Voice Cloning: What it is and why it's scary" (June 13, 2023), *available at* https://builtin.com/artificial-intelligence/what-is-voice-cloning.

[6] Under Attorney General's Consumer Protection regulations, "product" includes "goods, whether tangible or intangible, real, personal, or mixed, services, or franchise or distribution systems of any nature whatsoever." 940 Code Mass. Regs. 3.01.

in this Advisory, the AGO provides guidance that the following acts or practices are "unfair and deceptive" within the meaning of Chapter 93A, §2:[7]

It is unfair or deceptive to:

- Falsely advertise the quality, value, or usability of AI systems. 940 Code Mass. Regs. 3.02(2). An example of false advertising is where a supplier claims that an AI system has functionality that it does not possess.
- Supply an AI system that is defective, unusable, or impractical for the purpose advertised. 940 Code Mass. Regs. 3.02(4)(d). Suppliers have an obligation to ensure that an AI system performs as intended. *American Shooting Sports Council, Inc. v. Attorney Gen.,* 429 Mass. 871, 877 (1999) (the failure to meet fundamental performance standards is particularly "unfair" or "deceptive" where "harmful or unexpected risks or dangers inherent in the product, or latent performance inadequacies, cannot be detected by the average user or cannot be avoided by adequate disclosures or warnings.").
- Misrepresent the reliability, manner of performance, safety, or condition of an AI system. 940 Code Mass. Regs. 3.05(1). Examples of misrepresentation include claims or representations that an AI system is fully automated when its functions are performed in whole or in part by humans, as well as untested and unverified claims that an AI system performs functions with equal accuracy to a human, is more capable than a human at performing a given function, is superior to non-AI products, is free from bias, is not susceptible to malicious use by a bad actor, or is compliant with state and federal law.
- Offer for sale or use an AI system in breach of warranty in that the system is not fit for the ordinary purposes for which such systems are used, or that is unfit for the specific purpose for which it is sold where the supplier knows of such purpose. 940 Code Mass. Regs. 3.01; 940 Code Mass. Regs. 3.08(2); *Maillet v. ATF-Davidson Co.,* 407 Mass. 185, 193 (1990) ("Generally, a breach of warranty constitutes a violation of G.L. c. 93A, § 2.") For example, offering for sale or use an AI system that is not robust enough to perform appropriately in a real-world environment as compared to a testing environment is unfair and deceptive.
- Misrepresent audio or video content of a person for the purpose of deceiving another to engage in a business transaction or supply personal information as if to a trusted business partner as in the case of deepfakes, voice cloning, or chatbots used to engage in fraud. 940 Code Mass. Regs. 3.05 (1).[8]

[7] This list is not exhaustive. The Attorney General Office anticipates that this Advisory will be amended or expanded as AI systems and the laws that govern them continue to evolve.

[8] *See* Michael Atleson, "Chatbots, deepfakes, and voice clones: AI deception for sale," Fed. Trade Comm'n Business Blog (March 20, 2023), *available at* https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale ("The FTC Act's prohibition on deceptive or unfair conduct can apply if you make, sell, or use a tool that is effectively designed to deceive – even if that's not its intended or sole purpose.")

- Fails to comply with Massachusetts "statutes, rules, regulations or laws, meant for the protection of the public's health, safety or welfare." 940 Code Mass. Regs 3.16(3).

Additionally, AI suppliers are advised that it may be a violation of Chapter 93A, § 2 if an AI system is sold or used in a manner that violates federal consumer protection statutes, including the Federal Trade Commission Act. 940 Code Mass. Regs. 3.16(4). The Federal Trade Commission has taken the position that deceptive or misleading claims about the capabilities of an AI system, and the sale or use of AI systems that cause harm to consumers violate the Federal Trade Commission Act. *See, e.g.*, Fed. Trade Comm'n Report to Congress, "Combatting Online Harms Through Innovation" 2 (June 2022), *available at* https://www.ftc.gov/reports/combatting-online-harms-through-innovation; Michale Atleson, *Keep your AI claims in check,* Fed. Trade Comm'n Business Blog (Feb. 27, 2023), *available at* https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check. This includes any AI that impersonates a government, businesses, or their officials. *See generally* 16 CFR part 461 (April 1, 2024).

AI systems must also comply with the Commonwealth's Standards for the Protection of Personal Information of Residents of the Commonwealth, promulgated under Chapter 93H. This means that AI developers, suppliers, and users must take the necessary and appropriate steps to safeguard personal information used by those systems, *see* 201 Code Mass. Regs. 17.03 & 17.04, and are expected to comply with the breach notification requirements set forth in the statute. Violations of Chapter 93H are expressly subject to enforcement under Chapter 93A. G.L. c. 93H, § 6.

Furthermore, the Commonwealth's Anti-Discrimination Law, G.L c. 151B, § 4, prohibits developers, suppliers, and users of AI systems from deploying technology that discriminates against residents on the basis of a legally protected characteristic. This includes algorithmic decision-making that relies on or uses discriminatory inputs and that produces discriminatory results, such as those that have the purpose or effect of disfavoring or disadvantaging a person or group of people based on a legally protected characteristic. *See, e.g.*, *Lopez v. Commonwealth*, 463 Mass. 696, 709 (2012) ("G.L. c. 151B, § 4, like Title VII, proscribes not only overt discrimination but also practices that are fair in form, but discriminatory in operation."). Violations of Chapter 151B may constitute an unfair and deceptive act or practice, and thus may give rise to liability under Chapter 93A. *See* 940 Code Mass. Regs 3.16(3).

Finally, state attorneys general are also empowered to enforce certain federal consumer protection, anti-discrimination, and other laws applicable to AI. *See* 12 U.S.C. § 5481, 5552. For example, the adverse action notification requirements under the federal Equal Credit and Opportunity Act (ECOA), the primary federal law that prohibits discrimination in credit, applies to AI models. This means that covered creditors must provide accurate and specific reasons to consumers indicating why their loan applications were denied, including in circumstances where the creditor uses AI models. *See* Consumer Financial Protection Bureau Circular 2023-03, "Adverse Action Notification Requirements and the Proper Use of the CFPB's Sample Forms Provided in Regulation B" (Sept. 19, 2023).