CONSIDERATIONS

POLICY

Generative AI for Organizational Use:
Internal Policy Considerations

Future of Privacy Forum, updated June 2024

FUTURE OF PRIVACY FORUM

FPF
CENTER FOR ARTIFICIAL INTELLIGENCE

ACKNOWLEDGEMENTS

This document was made possible with the contributions of Amber Ezzell (Policy Counsel), Daniel Berrick (Policy Counsel), and Lael Bellamy (Senior Fellow). FPF would also like to thank Anne J. Flanagan, John Verdi, and the many experts and stakeholders who were consulted for their contributions to the report.

Executive Summary

As the use of generative AI increases, organizations are revisiting their internal policies and procedures to ensure responsible, legal, and ethical employee and vendor use of these tools. The Future of Privacy Forum previously consulted over 30 cross-sector practitioners and experts in law, technology, and policy to understand the most pressing issues and how experts are accounting for generative AI tools in policy and training guidance. FPF's Internal Policy Considerations are intended as a starting point for the development of organizational generative AI policies, highlighting areas in which organizations should develop and/or assess internal policies. The updated considerations include additional detail and guidance to consider. As always, this field is ever changing and this does not constitute legal advice.

Use AI in Compliance with Existing Laws and Policies for Data Protection and Security
Designated teams or individuals should revisit internal policies and procedures to ensure that they account for planned or permitted uses of generative AI. Employees must understand that relevant current or pending legal obligations apply to the use of new tools and technologies.

Specific Concerns and Enforcement By Regulators
Organizations that develop or use generative AI tools should be mindful of algorithmic disgorgement and use it to encourage internal compliance with legal requirements. It is also important to evaluate whether certain applications of generative AI systems either qualify as high-risk uses, or are prohibited under relevant laws, such as the EU AI Act.

Provide Appropriate Training and Education
Workers should be properly trained on the organization's policies and processes for acquiring and using these tools to ensure a proper understanding of:

- how the tools work (or do not work),
- the limitations of the tools and the outcomes, and
- the risks to the organization and to individuals.

Identified personnel should inform employees of the implications and consequences of using generative AI in the workplace, including providing training and resources on responsible use, risk, ethics, and bias.

Make Use Disclosures

Organizations should provide employees with clear guidance on the use of organizational accounts for generative AI tools, as well as policies regarding permitted and prohibited uses of those tools in the workplace. Designated leads should communicate norms around documenting use and disclosing when generative AI tools are used.

Analyze Outputs of Generative AI

Systems should be implemented to verify outputs of generative AI, including for issues regarding accuracy, timeliness, bias, regular review/notice or possible infringement of intellectual property, and other rights. When generative AI is used for coding, for example, appropriate personnel should check and validate outputs for security and other vulnerabilities.

Consider Ongoing Responsibilities

Privacy, data protection, and AI impact assessments are ongoing responsibilities that entail cross-team collaboration from across the organization. Employees using generative AI systems should be aware of public policy considerations—such as those related to addressing bias and toxicity—that override system outputs in order to mitigate or prevent the social and ethical harms that may arise from the deployment of generative AI systems. In addition to privacy counsel, organizations should engage with experts representing a variety of legal specialties to issue spot and identify appropriate mitigations.

Generative AI for Organizational Use: Internal Policy Considerations

June 2024

Introduction

Generative AI is a category of artificial intelligence that "generate[s] new outputs based on the data they have been trained on."[1] Large Language Models (LLMs) are a popular type of program that uses machine learning to generate and recognize text and other content. Most are trained on large amounts of foundational data scraped from online sources such as Wikipedia articles, books and other public webpages, some of which contain inaccurate, biased or personal information.[2] Generative AI has improved in a short period of time. However, it does not "understand" text—it predicts the next word in the context of the paragraph and other inputs. Employees should understand the limitations of the tools they are using in order to use AI in a responsible manner while employers should familiarize themselves with the terms and conditions of the tools they procure, and consult explanatory resources offered by generative AI vendors and other stakeholders including regulators where regulatory guidance exists. Generative AI tools can take on a myriad of useful tasks within organizations including drafting emails or computer code, outlining reports or blog posts, providing biographic information, performing customer service functions, generating images, and even writing scripts for popular television shows.[3]

As their general popularity increases, so does workplace use of generative AI tools. Workers are using such tools in every field, across specialties, and at all levels of employment; there are few jobs in which LLMs are not relevant in at least one application.[4] Accordingly, organizations must grapple with the legal and social risks, benefits, and long-term consequences of

[1] Nick Routley. "What is generative AI? An AI explains," *World Economic Forum* (Feb. 6, 2023), https://www.weforum.org/agenda/2023/02/generative-ai-explain-algorithms-work. Generative AI can be used in a variety of contexts, to include creating images, text, videos, code, audio, etc. S*ee generally* "The Privacy Expert's Guide to Artificial Intelligence and Machine Learning," *FPF* (October 2018), https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf.

[2] The right or under certain privacy regimes such as GDPR, the legal basis to process personal data for training LLMs and other AI remains up for debate. Shreya Johri, "The Making of ChatGPT: From Data to Dialogue," *Science in the News* (June 6, 2023), https://sitn.hms.harvard.edu/flash/2023/the-making-of-chatgpt-from-data-to-dialogue/

[3] *See, e.g.,* "Generative AI for legal professionals: Its growing potential and top use cases," *Thomson Reuters* (May 20, 2024), https://legal.thomsonreuters.com/blog/generative-ai-for-legal-professionals-top-use-cases/

[4] Annie Lowrey, "How ChatGPT Will Destabilize White-Collar Work," *The Atlantic* (Jan. 20, 2023), https://www.theatlantic.com/ideas/archive/2023/01/chatgpt-ai-economy-automation-jobs/672767/

organizational support and use of generative AI. Organizations are rapidly revisiting internal policies and procedures to ensure responsible, legal, and ethical use.

The Future of Privacy Forum's Internal Policy Considerations include:

- Use AI in Compliance with Existing Laws and Policies for Data Protection and Security;
- Specific Concerns and Enforcement By Regulators;
- Provide Appropriate Training and Education;
- Make Use Disclosures;
- Analyze Outputs of Generative AI; and
- Consider Ongoing Responsibilities.

FPF consulted with leaders across business sectors to learn more about how organizations are using generative AI across teams and in different contexts. We held a series of conversations that included more than 30 experts on technology, law, and policy to understand the most pressing issues and how experts are accounting for generative AI tools in policy and training guidance. The below considerations, which provides a catalog of considerations for the use of generative AI within organizations, is a result of these conversations.

This is a living document; new issues associated with the use of generative AI or LLMs are routinely discovered and refined. When use of generative AI tools within an organization is imminent or already occurring, time may be of the essence, and a comprehensive training program may not be feasible. In such cases, it is critical for key units and individuals to collaborate with all employees to understand how and why different teams may want to use these tools and, at a minimum, form a cross-functional team (e.g., privacy and compliance, human resources, legal, security, IT, procurement) to compile and clearly communicate a survey of acceptable and prohibited uses, a designated contact point for any uses that are not specifically accounted for, and a timeline for any future actions that may provide greater detail or clarity.

This list of considerations should be used as a starting point for this cross-functional team, or any other system an organization chooses, for more advanced conversations, as well as a gateway to address additional issues unique to a particular tool. Risk management within the context of generative AI models is also an area of ongoing exploration, as some companies have already highlighted the potential risks of their development and use of generative AI

systems.[5] We have not attempted to address critical issues such as continuous monitoring and testing, notice or consent, or governance and operational resiliency (i.e., ensuring that the organizations' leaders monitor use of AI and escalate appropriate issues to enable the board of directors to exercise appropriate oversight).[6]

Note: We use the term "employees" as inclusive of, but not limited to: full-time staff, part-time staff, contractors, interns, or any others providing services for any form of compensation. Organizations should adapt these recommendations to be most useful for their area or sector and different employees, and should be read in the context of those factors.

Use AI in Compliance with Existing Laws and Policies for Data Protection and Security

- ☐ Designated teams or individuals should revisit internal policies and procedures, including privacy policies, data use policies, security, information classification and management policies, and terms of service, to ensure that they account for planned or permitted uses of generative AI.
- ☐ Individuals or teams responsible for procurement, product review and development, and/or enterprise risk management should collaborate to develop criteria to assess and approve new or updated third party software and services that integrate with generative AI technology or offer generative AI features. Internal reviewers should consider the data sets used to create the outputs, as not all tools raise the same risks. Reviewers should also consider whether the organization should provide transparency to the public or impacted individuals regarding the organization's generative AI use.[7]
- ☐ Sharing data with vendors must be subject to requirements that ensure compliance with relevant U.S. and other laws, including U.S. state laws regulating the sharing or sale of

[5] *See* "GPT-4 System Card," *Open AI* (Mar. 23, 2023), https://cdn.openai.com/papers/gpt-4-system-card.pdf
[6] This resource also does not address the unique issues that organizations can encounter during the development , use or training of generative AI models and systems, such as possible intellectual property and privacy rights or legal bases to process the data used to develop and test models. *See* "Defining Governance in a Hybrid Word," *The Lares Institute* (Sept. 30, 2022), https://laresinstitute.com/wp-content/uploads/2023/09/Combined-LinkedIn-Posts.pdf; *See* "Understanding Delaware Fiduciary Duties—Putting Governance and Risk in Context and Reducing Personal Liability," *The Lares Institute* (Aug. 2023), https://laresinstitute.com/wp-content/uploads/2023/09/Delaware-Fiduciary-Duties-White-Paper.pdf.
[7] *See* "Generative AI: eight questions that developers and users need to ask," *Information Commissioner's Office* (Apr. 3, 2023), https://ico.org.uk/about-the-ico/media-centre/blog-generative-ai-eight-questions-that-developers-and-users-need-to-ask/

data.[8] Review contractual terms to ensure that any uses of data by vendors reflect mandatory state contractual language, or are subject to approved exceptions. Ensure appropriate consumer notices and/or consents and choices are in place and ensure the organization and vendors comply with other licensing and requirements such as data minimization, purpose limitation, profiling, use of sensitive or confidential information, including cooperation, testing, auditing and operational requirements to address relevant consumer rights and requests such as "Rights to Access, Correct and Delete," "Do Not Sell or Share," limitations or prohibitions on profiling, and requirements not to discriminate.

- ☐ Ensure vendors have the rights to process and provide the tools, data and services and will support any required notice, testing, auditing, requests.
- ☐ Current legal obligations apply to the use of all tools, including new ones, particularly in regard to internal policies, as well as applicable laws and regulations related to privacy and data protection, profiling and automated-decision making, data use, bias and discrimination, intellectual property, or other legal or policy frameworks of particular interest to the organization. As necessary, specific training may be useful as to how to mitigate legal liability in the use of generative AI. Uses with heightened risks may warrant prior review, including legal review.
- ☐ If an organization is part of a highly regulated industry, it should pay extra care to understanding and communicating any specialized legal obligations or liability. Rules should be considered for employees to ensure that they are not intentionally exposing their organization to liability. The organization should review guidance, where it exists, from relevant regulatory agencies on the use of generative AI, and incorporate that information into their internal policies and protocols.
- ☐ Employees should be advised to avoid inputting sensitive or confidential information, any trade secrets or other intellectual property, or any personal data into any generative AI prompt where it is not clear in the terms of service of the tool whether or not that data is protected. Employees should not prompt generative AI tools to output sensitive or confidential information. Sensitive or confidential information may include corporate trade secret information or data about users, competitors, clients, customers, employees, subscribers, or other individuals. Special care should be taken when

[8] Organizations should also be mindful of differences in legal requirements across jurisdictions, which can affect compliance obligations. *E.g.,* Dominic Paulger, "Navigating Governance Frameworks for Generative AI Systems in the Asia-Pacific," *FPF* (May 23, 2024), https://fpf.org/wp-content/uploads/2024/05/Navigating-Governance-Frameworks-for-Gen-AI-Systems-in-the-Asia-Pacific.pdf

handling children's data, education data, hiring or workplace data that could lead to claims of discrimination or harassment, and other regulated forms of data.

- ☐ When using generative AI applications on work-issued devices, employees should be advised as to recommended settings or permissions associated with the LLM or generative AI to ensure that data on that device is protected against unwanted access by the application. Employees should be reminded of prior data protection and security training to ensure that their devices and networks are secure in order to prevent unauthorized access to data.
- ☐ In 2021, the U.S. Equal Employment Opportunity Commission (EEOC) announced that it was launching an initiative on Artificial Intelligence and Algorithmic Fairness and stated "***While the technology may be evolving, anti-discrimination laws still apply.*** The EEOC will address workplace bias that violates federal civil rights laws regardless of the form it takes, and the agency is committed to helping employers understand how to benefit from these new technologies while also complying with employment laws."[9] True to its word, the EEOC has released a number of helpful resources. The EEOC brought its first enforcement action in 2023 against an employer using AI to discriminate against job applicants. The case was settled for $365,000, in addition to extensive compliance, employee notice, training, monitoring, reporting, and recordkeeping requirements.[10]

Consider Specific Concerns and Enforcement By Regulators

Beyond fines, enforcement bodies may pursue other remedies against companies that violate laws governing generative AI tools. In recent years, the Federal Trade Commission (FTC) has utilized algorithmic disgorgement—the requirement that companies delete all data, models, and algorithms resulting, in part or in whole, from unfair, deceptive, or otherwise unlawful trade practices, including use of data and/or images internally to train AI.[11] These cases cover multiple sectors and respond to different applications of AI, demonstrating regulators willingness to pursue this remedy across a variety of contexts to address perceived AI harms

[9] "EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness," *EEOC* (Oct. 28, 2021), https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness#:~:text=The%20EEOC%20will%20address%20workplace,also%20complying%20with%20employment%20laws.%E2%80%9D

[10] "iTutorGroup to Pay $365,000 to Settle EEOC Discriminatory Hiring Suit," *EEOC* (Sept. 11, 2023), https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit

[11] Jevan Hutson and Ben Winters, "America's Next 'Stop Model!': Model Deletion," *Georgetown Law Tech. Rev.* (Sept. 20, 2022), https://ssrn.com/abstract=4225003.

and violations of law.[12] Organizations that develop or use generative AI tools should be mindful of this enforcement tool and use it to encourage internal compliance with legal requirements.

Organizations need to evaluate whether certain applications of generative AI systems either qualify as high-risk uses, or are prohibited under relevant laws, such as the EU AI Act. This analysis is important to determine whether additional obligations attach to the use of a generative AI system, which in turn may impact the contents of internal use policies. EU regulators are not the only ones at the forefront of enforcement. Four U.S. federal agencies, the Consumer Financial Protection Bureau (CFPB), the Department of Justice's Civil Rights Division, the EEOC, and the FTC, issued a joint statement on the use of automated systems, including AI, and the applicability of existing law to new technology including for the "the enforcement of civil rights, non-discrimination, fair competition, consumer protection, and other vitally important legal protections."[13]

Provide Appropriate Training and Education

- ☐ Organizations should inform employees about the implications and consequences of using generative AI tools in the workplace. Organizations should review and understand the generative AI system's contractual terms, intended uses, and other relevant materials, including privacy policies, documentation, and responsible AI program, to understand how personal data is handled, processed, and protected. If there are specific generative AI tools that the organization wishes to recommend, discourage use of, or issue special warnings for, be sure to communicate that clearly and affirmatively.
- ☐ Organizations must identify risks of using generative AI in context, including legal, regulatory, or ethical obligations, as well as potential liabilities associated with the use of generative AI tools. Organizations should provide employees with new or existing resources that advise about the responsible use of any automated processing tool. Existing educational resources should be updated where possible to expressly address generative AI tools. Relevant training and workshops may include, but are not limited to,

[12] *See, e.g.,* "FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay $16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking," *FTC* (Feb. 22, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over (requiring Avast to delete the web browsing information transferred to Jumpshot and any products or algorithms Jumpshot derived from that data.").
[13] "Joint Statement on Enforcement of Civil Rights, Fair Competition, Consumer Protection, and Equal Opportunity Laws in Automated Systems," *EEOC* (Apr. 3, 2024), https://www.eeoc.gov/joint-statement-enforcement-civil-rights-fair-competition-consumer-protection-and-equal-opportunity

training on ethics, bias, data inaccuracy, security concerns, intellectual property rights, confidential information, and data minimization.

- ☐ Software developers and data scientists using generative AI models should be trained on ethics, bias, data inaccuracy, security concerns, intellectual property impacts, trade secrets, and data minimization.
- ☐ Governance programs should be established to address risks and legal restrictions related to high-risk profiling and automated decision-making, as well as key data protection principles such as data minimization, purpose limitation, limitations on processing of sensitive personal data, and privacy by design and by default.
- ☐ Given the speed at which generative AI is developing, leadership at organizations should designate personnel responsible for staying abreast of regulatory and technical developments and ensure that company policies and employee practices reflect such changes. The contact information for these personnel should be available to all employees, and employees should be reminded of the appropriate points of contact for the organization's privacy and/or data protection policies (e.g., data protection officers) should they have any questions or concerns about the use of generative AI. Some organizations concentrate this function in IT, Legal or Human Resources while others charge internal AI governance committees with the function.

Make Use Disclosures

- ☐ Organizations should establish policies for how employees use AI services or tools. Employees should only use generative AI tools or systems that have been approved by the organization for specific use cases or purposes.
- ☐ Accountability for the use of generative AI may require that employees have access to a system to document their use of these tools for business purposes.
- ☐ Organizations should require employees to disclose whether internal and/or external work product was created in whole or part by generative AI tools.
- ☐ Organizations should recognize the creative approaches that many employees will take to use generative AI tools at work. Typically, organizations should publish approved and prohibited use cases and direct employees how to submit new use cases for review. Organizations should update internal documentation, including employee handbooks and related policies, to reflect policies regarding generative AI uses.

Analyze Outputs of Generative AI

- ☐ Employees should be trained that: generative AI outputs can be incorrect, out-of-date, biased, or misleading. Individuals are responsible for the content they create, regardless of the assistance of generative AI tools, and employees are encouraged to independently verify the accuracy of any outputs. Independent verification is particularly important if employees use AI in situations that require legal certification of accuracy, e.g., financial reports, court filings, and due diligence documents.
- ☐ Employees should understand that content used to teach generative AI tools may be subject to copyright protections or implicate holders of intellectual property. Depending on the circumstance, organizational leadership may also advise employees to refrain from using AI-generated content if there is a question about intellectual property rights. The organization should decide whether, to what extent, and in what situations, including if there is direct use, derivative use, or when it is clear that the material was a source for the output.
- ☐ Coding outputs by generative AI should be checked and validated for security and other vulnerabilities. Some AI tools can be trained to generate output based on the quality of the existing code or the skills of the coder—as is true in most situations, garbage in, garbage out.

Consider Ongoing Responsibilities

Organizations using generative AI systems or making updates to them may have to perform privacy, data protection and AI impact assessments, test, and audit these systems. While privacy and data protection impact assessments (DPIAs) are not new, recently passed laws requiring assessments specifically tailored to the risks posed by AI systems are.[14] These are not one-off obligations; organizations need to perform them on an ongoing basis.[15] Similarly, testing and auditing of generative AI systems, which are key parts of responsible AI

[14] Colorado AI Act, § 6-1-1703 (3)(a) (2024).
[15] *Id.* at § 6-1-1703 (3)(a)(I)–(II) (requiring that deployers or high-risk AI systems complete impact assessments for these systems every year and within 90 days of any intentional and substantial modification to the system being made available).

governance, are ongoing responsibilities that entail cross-team collaboration from across the organization.[16]

As organizations deploy generative AI systems tools to diverse contexts, employees seek to balance the outputs of these systems with legal requirements, values, and other policies. Employees using generative AI systems should be especially mindful of public policy considerations (e.g., anti-bias and toxicity) that seek to mitigate or prevent social and ethical harms, which may arise from the deployment of generative AI systems. These considerations may override the outputs of these systems, notwithstanding the output's accuracy. In addition to public policy considerations, organizations deploying generative AI systems should evaluate the myriad legal issues that these systems can raise beyond privacy compliance. This underscores the importance of engaging with experts representing a variety of legal specialties to issue spot and identify appropriate mitigations.

Resources

1. Regulation of AI
    a. FTC guidance regarding generative AI. Note in particular the Commission's warnings about representations of accuracy.
        i. Chatbots, deepfakes, and voice clones: AI deception for sale[17]
        ii. The Luring Test: AI and the engineering of consumer trust[18]

[16] *See* "Responsible Use of Machine Learning Version 1.2," *AWS* (June 21, 2023), https://d1.awsstatic.com/responsible-machine-learning/AWS_Responsible_Use_of_ML_Whitepaper_1.2.pdf (describing how it is important for organizations to test machine learning systems in each environment they will operate them, including on the data on which they will be deployed before going live); "What is AI Governance?" *IBM* (Nov. 28, 2023), https://www.ibm.com/topics/ai-governance#:~:text=Artificial%20intelligence%20(AI)%20governance%20refers,and%20remain%20safe%20and%20ethical. (noting that "[a]udit teams are essential for validating the data integrity of AI systems and confirming that the systems operate as intended without introducing errors or biases . . . [but] responsibility for AI governance does not rest with a single individual or department.").
[17] https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale
[18] https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust

iii. Keep your AI claims in check[19]

b. GPT, GDPR, AI Act: How (Not) To Regulate "Generative AI?" (NYU Law, April 24, 2023)[20]

2. Understanding Generative AI
    a. Exploring Generative AI and Law: ChatGPT, Midjourney, and Other Innovations | Pre-Conference Primer (Professor Harry Surden, Silicon Flatirons)[21]
3. Managing Risk
    a. Managing the risks of generative AI - A playbook for risk executives – beginning with governance (PWC)[22]
4. Emerging EU Guidance
    a. Although this document is primarily intended for a US audience, emerging guidance from EU regulators is useful for US and global audiences. Generative AI: eight questions that developers and users need to ask (ICO, April 3, 2023)[23]

For more information please contact the FPF Center for Artificial Intelligence at ai@fpf.org.

[19] https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check
[20] https://www.guariniglobal.org/gpt-conference-materials
[21] https://www.youtube.com/watch?v=RRzMSKzUh6A
[22] https://explore.pwc.com/generativeai?_pfses=D8nsC9bP5NQMW25zxpYx69tC
[23] https://ico.org.uk/about-the-ico/media-centre/blog-generative-ai-eight-questions-that-developers-and-users-need-to-ask/

FPF.org