CHECKLIST

POLICY

Generative AI for Organizational Use:

Internal Policy Checklist

Amber Ezzell, Future of Privacy Forum, July 2023

FUTURE OF PRIVACY FORUM

Executive Summary

As the use of generative AI increases, organizations are revisiting their internal policies and procedures to ensure responsible, legal, and ethical employee use of these novel tools. The Future of Privacy Forum 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 Checklist is intended as a starting point for the development of organizational generative AI policies, highlighting four areas in which organizations should develop and/or assess internal policies. The full checklist includes additional detail and guidance.

Use 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.

Employee Training and Education
Identified personnel should inform employees of the implications and consequences of using generative AI tools in the workplace, including providing training and resources on responsible use, risk, ethics, and bias. Designated leads should provide employees with regular reminders of legal, regulatory, and ethical obligations.

Employee Use Disclosure
Organizations should provide employees with clear guidance on when and whether to use 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.

Outputs of Generative AI
Systems should be implemented to remind employees to verify outputs of generative AI, including for issues regarding accuracy, timeliness, bias, or possible infringement of intellectual property rights. Organizations should determine whether and to what extent compensation should be provided to those whose intellectual property is implicated by generative AI outputs. When generative AI is used for coding, appropriate personnel should check and validate outputs for security vulnerabilities.

Generative AI for Organizational Use: Internal Policy Checklist

July 2023

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 generative AI that generates responses to natural language queries. Examples include Google Bard and Open AI's ChatGPT (chatbots), Microsoft's AI-powered Bing (search engine), Midjourney's Midjourney and Open AI's DALL-E (image generators). Generative AI tools can draft emails or computer code, outline reports or blog posts, provide biographic information, perform customer service functions, generate images, and write scripts for popular television shows.[2]

As their general popularity increases, so does workplace use of generative AI and LLMs. Workers are using generative AI 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.[3] Accordingly, organizations must grapple with the legal and social risks, benefits, and long-term consequences of organizational support and use of generative AI. Organizations are rapidly revisiting internal policies and procedures to ensure responsible, legal, and ethical use. 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), risks to the organization if they are not properly acquired or used, and their limitations.

The Future of Privacy Forum's checklist provides guidance regarding:

- Use in Compliance with Existing Laws and Policies for Data Protection & Security;
- Employee Training and Education;
- Employee Use Disclosure; and
- Outputs of Generative AI

---

[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] *See, e.g.,* https://www.iflscience.com/south-park-creators-use-chatgpt-to-co-write-episode-about-ai-68059.

[3] 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/

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 checklist, 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, etc.) 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 full checklist should be considered 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 organization or field. 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 generative AI systems.[4]

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 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, information classification and management policies, and terms of service, to ensure that they account for planned or permitted uses of generative AI.

[4] *See* "GPT-4 System Card," *Open AI* (Mar. 23, 2023), https://cdn.openai.com/papers/gpt-4-system-card.pdf

- ☐ Individuals or teams responsible for procurement 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 APIs 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.[5]
- ☐ Sharing data with vendors must be subject to requirements that ensure compliance with relevant US state laws regulating sharing or sale of data. Review contractual terms to ensure that any uses of data by vendors reflect mandatory state contractual language, or are subject to approved exceptions. If use of data by a vendor is deemed sharing or sale, ensure appropriate consumer notices are in place and ensure the organization and vendors comply with relevant consumer requests such as "Do Not Sell" requests.
- ☐ Ensure vendors will support any required access and deletion requests.
- ☐ Managers should remind all employees that relevant current or pending legal obligations will continue to apply to the use of new tools, particularly in regard to internal policies as well as applicable laws and regulations related to privacy and data protection, 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 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 into a generative AI prompt unless data is processed locally and/or subject to appropriate controls regarding access or use. Employees should not prompt generative AI tools to output sensitive or confidential information unless data is processed locally and/or

[5] *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/

subject to appropriate controls regarding access or use. 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 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.

Employee 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 terms of use and other relevant materials, including privacy policies, 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, training on ethics, bias, data inaccuracy, security concerns, intellectual property rights, confidential information, and data minimization.
- ☐ Software developers and data scientists accessing generative AI models through APIs or building applications that use these models should be trained on ethics, bias, data inaccuracy, security concerns, intellectual property impacts, trade secrets, and data minimization.
- ☐ A system should be established to regularly remind individuals of legal restrictions on profiling and automated decision-making, as well as key data protection principles such

as data minimization, purpose limitation, limitations on sale of personal data, and privacy by design and by default.

- ☐ Given the speed at which generative AI technologies are 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 tools.

Employee Use Disclosure

- ☐ Organizations should establish policies for how employees should sign up to use generative AI tools that require account creation, including whether the organization requires or prohibits the use of organizational email accounts for particular AI services or uses. Employees should only use generative AI tools or systems that have been approved by the organization.
- ☐ 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. Such tools should be easy to use, enable employees to add context around any use, and provide a method to indicate how that use fits into the organizations' policies. For example, organizations may require employees to download and retain chat transcripts and prompts.
- ☐ Organizations should communicate when and how the organization will 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 professional use of generative AI tools. Typically, organizations should not create blanket bans on use by job title (e.g. HR employees), but rather provide employees with clear guidance on how they can or cannot use generative AI tools to perform their essential job functions (e.g. restricting or prohibiting HR employees from inputting employee names, addresses, social security numbers, etc. into ChatGPT). Organizations should update internal documentation, including employee handbooks and related policies, to reflect policies regarding Generative AI use.

Outputs of Generative AI

- ☐ Employees should be regularly reminded 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. Verification is particularly important when employees use AI in situations that require legal certification of accuracy, e.g. financial reports, court filings, and due diligence documents.
- ☐ Employees should be advised that content from 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, it is determined that compensation should be provided to those whose intellectual property is implicated by the output of a generative AI, 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 vulnerabilities.

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[6]
        ii. The Luring Test: AI and the engineering of consumer trust[7]
        iii. Keep your AI claims in check[8]
    b. GPT, GDPR, AI Act: How (Not) To Regulate "Generative AI?" (NYU Law, April 24, 2023)[9]
2. Understanding Generative AI
    a. Exploring Generative AI and Law: ChatGPT, Midjourney, and Other Innovations | Pre-Conference Primer (Professor Harry Surden, Silicon Flatirons)[10]
3. Managing Risk
    a. Managing the risks of generative AI - A playbook for risk executives – beginning with governance (PWC)[11]
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)[12]

For more information please contact FPF Policy Counsel Amber Ezzell at aezzell@fpf.org or info@fpf.org.

[6] https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale
[7] https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust
[8] https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check
[9] https://www.guariniglobal.org/gpt-conference-materials
[10] https://www.youtube.com/watch?v=RRzMSKzUh6A
[11] https://explore.pwc.com/generativeai?_pfses=D8nsC9bP5NQMW25zxpYx69tC
[12] https://ico.org.uk/about-the-ico/media-centre/blog-generative-ai-eight-questions-that-developers-and-users-need-to-ask/

FPF.org