WILSON
SONSINI

Generative AI: Privacy and Consumer Protection Considerations

CONTRIBUTORS

Maneesha Mithal

Nikhil Goyal

ALERTS

May 26, 2023

Generative AI (GenAI) has been at the top of the headlines lately, transforming fields as varied as journalism, marketing, and gaming, boosting productivity and profitability, and performing functions previously limited to humans. Recent projections suggest that the global GenAI market will increase to over $100 billion annually by 2030. A previous Wilson Sonsini alert on GenAI covered a wide range of issues, such as breach of contract, confidentiality, copyright, ethics, European Union laws and regulations, licensing, securities laws, trade secrets, and reputational considerations. Another previous alert addressed legal requirements for mitigating bias in AI systems more generally. This alert drills down on U.S. privacy and consumer protection considerations associated specifically with GenAI.

GenAI technology tools are developed and refined by training the underlying models on large training data sets that are drawn from a number of sources, and can include personal information from employees, website visitors, customers, and public sources, potentially creating risks under U.S. privacy and consumer protection laws. This alert is focused on identifying the key U.S. privacy and consumer protection-related risks associated with the use and creation of GenAI, along with steps companies can take to mitigate these risks.

A Primer on Applicable Laws

The use of GenAI implicates various privacy and consumer protection laws and regulatory considerations. Potentially applicable legal requirements include:

- **Prohibitions on Deceptive Practices:** The FTC Act and corresponding state laws generally prohibit deceptive practices. For example, if a company were to make inaccurate representations about how its AI uses training data to build models, that could be a deceptive practice. If a company uses chatbots or deepfakes to impersonate someone in a way that misleads consumers, that could also be deceptive. And some laws require affirmative disclosures to avoid deception. For example, California law requires a clear and conspicuous disclosure designed to inform consumers that they are interacting with an AI bot, when the AI bot is being used to incentivize a sale or transaction of goods or services or to influence a vote in an election.
- **Prohibitions on Unfair Practices:** The FTC has also issued guidance suggesting that failure to protect against reasonably foreseeable misuse of GenAI tools could be an unfair practice. For example, it has advised that, in addition to not using technologies to mislead consumers, companies releasing GenAI tools that allow use of deepfakes and chatbots should take steps before launch to deter the use of these technologies by fraudsters.
- **Privacy Laws:** There are numerous ways GenAI tools might use personal information. They may use queries input by employees, website visitors, or customers, which could include personal information, to train and refine their models. They may have been trained on data scraped from

the Web or government sources, which may contain information about consumers. They may use customer interactions on specific apps, websites, or with customer service personnel or monitor how customers use an app or internet-connected product. They may also use location data from someone's phone. Numerous generally applicable state privacy laws apply in these situations, governing collection, use, and disclosure of information in a variety of contexts. There are also laws targeted at the privacy of particular populations, such as the federal Children's Online Privacy Protection Act (COPPA), which applies to website or online services directed to children under 13, and the California Age Appropriate Design Code (AADC), effective on July 1, 2024, which will require websites and online services likely to be accessed by children under 18 to develop a data protection impact assessment, in addition to other requirements. Laws requiring notice and opt-in consent for biometric information in Illinois and health information in Washington (with health information being broadly defined) include private rights of action. To the extent companies use sensitive children's or teens' data, biometric information, or health data in GenAI tools, they should take special care to comply with these laws.

- **Forthcoming AI Legislation:** Although, so far, the U.S. has not passed GenAI-specific laws, this technology is in legislators' crosshairs. The Senate Subcommittee on Privacy, Technology, and the Law held a high-profile hearing on regulation of AI on May 16, 2023. Two days later, on May 18, Senator Michael Bennet introduced a bill proposing the creation of a Federal Digital Platform Commission that would have the authority to make regulations concerning the use of personal information to generate content or to make decisions. States are also likely to jump into the fray.

With all of this activity, what should companies do? This alert provides separate guidance for companies that are using GenAI tools, and companies that are building GenAI tools.

What Should Companies Building GenAI Tools Do Now?

- **Inventory data inputs:** Conduct an inventory of personal information you use to build your GenAI tools. This will help you assess potential compliance obligations. Do you use data of employees, customers, or website visitors? If so, what types of data are you collecting? Keystroke data from open field inputs? Videos uploaded from customers? Chat threads? Audio recordings? Pay particular attention when using sensitive information in your tools, such as biometric information, health information, or children's information, in which case, additional requirements may apply.
- **Pay special attention if you use web scraping technologies:** Specific legal considerations may apply to scraping data from the Web or other public sources. Our prior alert discusses those considerations in more detail.
- **Assess reasonably foreseeable risks related to your GenAI tools:** Companies should assess how their tools could be used to help users commit fraud or engage in other harm to consumers. Could someone use your GenAI tools to develop imposter scams or engage in financial fraud through the use of deep fakes or voice clones? If so, in addition to warning users about misusing your GenAI systems, you may want to test and implement security measures and features pre-launch. Once you release your GenAI system, consider monitoring usage and take action to address misuse that harms consumers.
- **Review your claims:** Make sure you can substantiate all of your representations. Do not exaggerate the accuracy of your tools.
- **Implement procedures to comply with state privacy laws:** Conducting your data inventory can help you map out a compliance plan. Figure out the situations in which you are 1) a controller/business that determines the purpose and means of processing personal data (where, for example, consumers might be interacting with you directly); or 2) a processor/service provider, where you're providing tools and collecting personal information on behalf of another business that is interacting with the consumer. Different requirements will likely apply. Both controllers and processors will need to make sure they're accurately disclosing their data collection, use, and disclosure practices in a privacy policy. Depending on the data you collect and whether you are a controller or processor, you will have to figure out what data subject rights you need to provide, such as the right to opt in or opt out of data collection. Some state laws require you to conduct a data protection impact assessment in certain circumstances.
- **Apply general advertising law principles to ad-supported GenAI tools:** To the extent you are placing advertising within GenAI features, those ads should be clearly labeled as ads. Any GenAI output should distinguish clearly between what is organic and what is paid. People should know if a GenAI product's response is steering them to a particular website, service provider, or product because of a commercial relationship.
- **Monitor business and legal changes:** Consider conducting periodic monitoring and audits regarding the use of GenAI to identify any new uses of personal information that might trigger new legal requirements. Given the interest U.S. regulators have been expressing in AI issues, companies should also monitor changes to legal requirements including by signing up for Wilson Sonsini's client alert mailing list.

What Should Companies Using GenAI Tools Be Doing?

Companies that are not building GenAI tools may nonetheless want to use the services of companies providing these tools. They may want to include chatbots or GenAI-enabled search features on their own websites or online services. They may want to enable their employees to use these tools for business purposes. Or they may want to use GenAI tools to customize ads to specific people or groups. All of the same considerations discussed above will likely apply in these scenarios. Here are some additional considerations:

- **Understand what customer personal information will be shared with the GenAI tool:** As with the companies building GenAI services, it is important to understand what personal information (if any) you will be sharing with the GenAI tool, so you can make accurate representations and implement appropriate compliance measures, including consent, data subject access rights, and data protection impact assessments. In particular, the California Consumer Privacy Act specifically protects the privacy of employee information, so it is important to consider your obligations under that law.
- **Be careful about yours and your employees' use of GenAI tools:** For example, passing on results generated through a GenAI tool without substantiation as to their accuracy could be a deceptive practice. Likewise, make sure your employees are not sharing personal information of your customers with GenAI tools that aren't intended for processing personal information.
- **To the extent you use GenAI tools to build advertising or advertising campaigns, make sure they are not deceptive or misleading:** For example, using celebrity deepfakes to promote brands could be considered a violation of the FTC Act. Likewise, GenAI tools are known to create content that sounds convincing but isn't accurate. If you use such tools to create advertising content that includes product claims, make sure those claims are adequately substantiated.
- **If you use GenAI tools to provide content to children or teens, follow requirements related to age-appropriate design:** As noted above, once effective in 2024, California's AADC will apply broadly to services likely to be accessed to children under 18. Consider whether your service is likely to attract this audience. If so, you may have to conduct your own data protection impact assessment to assess what data you collect (either directly or through the AI tool) and its potential impact, and provide clear, age-appropriate disclosures, among other obligations.
- **Evaluate use of personal information:** Evaluate companies' claims regarding their GenAI models. For example, if they claim that no personal information is used to train their models, ask how they can be sure if consumers can submit open field inquiries. Ask what de-identification techniques they are using.
- **Include contractual restrictions:** Under state privacy laws, businesses are required to impose contractual restrictions on service providers that process personal information on their behalf. In some states, they must also enter into contracts with third parties to whom they "sell" personal information (with the term "sale" defined broadly). Determine whether the operator of the GenAI tool you are using is a service provider who may only use the information you share with them for specific and limited purposes (which cannot include targeted advertising), or a third party that may use the information more freely, in which case, you may be subject to more onerous compliance requirements.

The legal landscape concerning GenAI is changing quickly. Companies should carefully evaluate their use of GenAI models in the context of obligations and limitations imposed by U.S. privacy and consumer protection laws and regulations. Wilson Sonsini Goodrich & Rosati routinely helps companies navigate complex privacy and data security issues. For more information or advice concerning your compliance efforts related to GenAI, please contact Maneesha Mithal, Laura De Boel, Scott McKinney, Barath Chari, Eddie Holman, Nikhil Goyal, or any member of the firm's privacy and cybersecurity practice or artificial intelligence and machine learning working group.