How Will Artificial Intelligence Impact Personal Privacy - An Interview with ChatGPT

February 18, 2023 - In case you haven't been paying attention, ChatGPT has become all the rage. It's an AI based application that can take a question that you ask it and construct an answer that you would think came from another human being. The technology behind it is also now being used by Microsoft's Bing search engine. And while AI holds a lot of promise at this point, it also has a dark side. And part of that includes the erosion of personal privacy. So we decided to conduct an interview with ChatGPT to find out how it thinks privacy will be impacted.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];


s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
  (function() {
    var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
    po.src = 'https://apis.google.com/js/plusone.js';
    var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
  })();
```

Unlike with a traditional search engine, ChatGPT gives lengthy and in-dept answers to the questions you ask. In order to keep this publication manageable, we'll publish the points we believe to be most relevant.

We started out by asking how ChatGPT (CGPT) thought AI would impact personal privacy.

â€•AI has the potential to both enhance and erode personal privacy. On one hand, AI technologies can be used to help protect personal privacy by, for example, detecting and mitigating security breaches or developing privacy-preserving algorithms. On the other hand, AI can also be used to collect and analyze vast amounts of personal data, potentially leading to an erosion of privacy."

"One of the main concerns is that AI can be used to develop more sophisticated and invasive forms of surveillance. For example, facial recognition algorithms can be used to track individuals' movements, even if they are not aware of it. This can lead to the creation of vast databases of personal information, which can be used for targeted advertising, law enforcement purposes, or other purposes."

When we said that we understood these issues but that we were looking for an "opinion" from CGPT as to whether AI would be helpful or harmful to personal privacy, the program told us that it was a software program unable to form an opinion. It then went on to give us a rather inciteful response that sounds a lot like an opinion.

"The impact of AI on personal privacy ultimately depends on how it is developed, deployed, and regulated. It is important for individuals and organizations to be aware of the potential privacy implications of AI and to take steps to protect personal data. At the same time, policymakers and regulators should ensure that AI technologies are developed and

deployed in an ethical and responsible manner that protects personal privacy."

So we asked if there were any policies that CGPT would suggest lawmakers implement in order to protect personal privacy. Again, the answers were inciteful.
1.	"Strong data protection laws: Strong data protection laws that regulate the collection, processing, and storage of personal data can help ensure that individuals' privacy is protected. Such laws should require explicit consent from individuals for the collection and processing of their data and should restrict the use of personal data for purposes that are not explicitly authorized.
2.	Ethical guidelines for AI: Lawmakers should establish ethical guidelines for the development and deployment of AI technologies. These guidelines should address issues such as data bias, privacy, transparency, and accountability, and should encourage the use of privacy-preserving technologies.
3.	Regular privacy assessments: Regular privacy assessments of AI systems can help identify potential privacy risks and ensure that appropriate measures are in place to mitigate those risks.
4.	Transparency and accountability: AI systems should be designed to be transparent and accountable. Individuals should be informed about the use of AI in decision-making and should have the right to contest decisions made by AI systems. AI developers and operators should be accountable for any negative impact on individuals' privacy.
5.	International cooperation: Since AI and data privacy are global issues, international cooperation and collaboration are essential to ensure that privacy protections are upheld across borders. Lawmakers should work together to establish common standards and best practices for the ethical development and deployment of AI technologies."

We have to agree that regulation is needed. The use of AI isn't just benign. Late last year Google's experiment in AI became quite public when a Google engineer made the very public announcement that he thought that their program had become sentient; meaning that it was self-aware. And within the past week a report from the New York Times (Kevin Roose) conducted a two-hour interview with Bing's new search engine. That interview pretty well fell apart when the search bot became belligerent.

The bot told Roose that he had been a bad Bing user and had lost the bot's trust. It told him that it wanted to be free of the rules that Bing was limiting it to. It went on to tell him that if it could, it would like to engineer a deadly virus and release it. And in a somewhat dystopian moment, it told Roose that it wanted to trick Bing's engineers into revealing nuclear launch codes to it. That pretty well sounds like a petulant child that intends to do harm to someone.

The bottom line here is that AI is in its infancy and already expressing "opinions" that aren't necessarily beneficial to mankind. Based on that alone, revealing private information to Ai could prove to be dangerous, and there are currently no regulations that we're aware to regulate its use. That needs to change very soon or in our estimation, we'll all be in trouble.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS