KAUFMAN | DOLOWICH

"Advancing AI Technology: Ripe Ammunition for Unprecedented Lawsuits," published in Corporate Counsel, authors Jack Kallus, Esq. & Labeed Choudhry, Esq., 5-11-2023

For a number of years, Artificial Intelligence, or AI, has been helping job seekers refine their resumes, assisting students with their homework, and helping friends and neighbors with their side-hustles on social media. AI is a powerful tool that is helping millions of people make their lives more efficient. However, as with most well-intentioned advances in society and technology, AI is already having negative unintended consequences.

One such unintended consequence is the use of AI to assist cyber-criminals in hacking passwords. Enter PassGAN, an AI tool that can crack 51% of common passwords in less than a minute and 71% of common passwords in less than a day. A new study by Home Security Heroes details how PassGAN can achieve this incredible result by learning from the collection of real passwords exposed in past data breaches and using that information to crack current passwords. While passwords released in a hack or data breach from years ago may be otherwise useless alone, PassGAN takes what was otherwise dormant data and uses it to crack current passwords. The report acknowledges that this development “is a serious threat” to online security.

AI like PassGAN is a tool that many familiar with this technology have been forecasting for some time. In fact, Cameron F. Kerry, former Secretary for the U.S. Department of Commerce and known information technology thought leader, stated in his article Protecting Privacy in an AI-Driven World, “As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed.” (Brookings, Feb. 10, 2020). PassGAN is just the latest realization of this progression in technology.

The ripples caused by these technological advances and the continued proliferation of AI tools in the real world will be more widely felt soon enough in the legal realm and will undoubtedly require changes to the current state of U.S. privacy laws, especially as it relates to sustaining a private right of action based on a data breach. Currently, the test to whether a person is allowed to bring a lawsuit in Federal Court based on a data breach is based on three factors: (1) Whether a person’s data has been exposed as the result of a targeted attempt to obtain that data; (2) Whether any portion of the dataset has already been misused, such as through identity theft or fraud, even if the person looking to sue has not yet felt a direct impact of the breach; and (3)Whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud. These factors, known as the McMorris factors, were established by the Second Circuit on April 21, 2021, in the case of McMorris v. Carlos Lopez & Assoc.

Several recent cases however applying the McMorris factors have found the plaintiffs have no standing for lack of damages because there has not been specific misuse of their particular data. The Supreme Court, in its TransUnion v. Ramirez 2021 decision, goes even further, appearing to significantly reduce the viability of lawsuits premised on risk of future harm if there is no specific misuse of the plaintiffs’ own data. The premise of the TransUnion decision, and other decisions in a similar vein, is that unless a plaintiff can show an actual misuse of their own data, there is no actual injury, thus no standing, and thus no lawsuit.

However, the proliferation of AI such as PassGAN is likely to cause a stir in this analysis and likely require that this analysis be re-considered. As noted above, part of the learning process for PassGAN was to use actual passwords that were leaked in data breaches. By the very nature of their operation, AI such as PassGAN work best when they are fed entire data-sets. As such, if there is a data breach and that data is used to train an AI program, every person whose data was disclosed could argue that their individual data has been misused. Does the mere fact that an individual’s data was leaked and used to train hacking AI software confer standing? What if it’s not used to train hacking AI like PassGAN but is used to train some other type of AI, such as face-recognition AI or marketing AI? These are all questions that can disturb the current state of the law.

There is yet another consideration at play with the widespread prevalence of AI that is being overlooked. Generally speaking, most statutes and regulations that deal with data privacy focus on protecting PII, or Personally Identifiable Information, such as names, social security numbers, addresses or other discrete data that can be directly linked to a person, even with the use of a computer. However, AI is being constantly trained to use limited information to find hidden links. Therefore, information that was not considered PII because there was no direct link between the information and an individual before may suddenly become PII when analyzed by highly developed

AI software. In fact, past data breaches that revealed "personal information" but did not tie that information directly to individuals could have been thought of as "harmless." However, AI can now potentially aggregate information revealed from multiple "harmless" breaches to find links and PII where none was thought to exist. The rise of AI will require policymakers to either significantly expand the definition of PII or simply abandon the concept altogether if no longer a sufficient standard-bearer. At the end of the day, the increased proliferation and sophistication of AI may leave no choice but to assume that all personal information is PII.

In the meantime, lawsuits that were previously dismissed for lack of standing could potentially be revived if it can be shown that information disclosed from previously breached data was used to train an AI module. Data breaches that did not disclose what was then defined as PII will probably be looked at anew to determine whether the use of AI renders the disclosed data PII. Savvy plaintiff's attorneys may also argue that running their client's data through an AI mechanism is a new and separate injury that re-sets the statute of limitations, similar to how each missed mortgage payment re-sets the statute of limitations for foreclosure actions. Therefore, data breach lawsuits that may have been otherwise time-barred could now be brought. If running a person's data through a malicious AI program is indeed an injury in itself, then cases that were previously dismissed due to lack of injury, and therefore standing, could suddenly be revived.

Policymakers have long been able to brush aside the call for greater regulation in this space such as the warnings issued in the Brookings Report referenced above, and regulators have been playing a game of chicken with this issue for years, continuously kicking this can down the road. However, the march of technology is unyielding, and it is now time to make difficult policy decisions because the road used to kick the can is now at a dead end.

While Legislators and regulators dilly-dally over what to do about the pressing issue of privacy laws, the Plaintiffs Bar is unlikely to sit still and simply wait for them to act. Legislation is required to provide guidelines on these issues for the courts so that when these issues are litigated, they can be decided in a uniform manner. If there is no clear and uniform regulation on these issues soon, there is potential for chaos as these issues are decided in piecemeal in courts across the country.

Jack Kallus is a Commercial Litigation partner in the Fort Lauderdale, Fla. office of Kaufman Dolowich & Voluck, LLP. He represents businesses and private wealth clients in a range of litigations including in matters pertaining to data security and privacy. Labeed Choudhry is a Commercial Litigation associate in the Fort Lauderdale, Fla. Office of Kaufman Dolowich & Voluck, LLP. He litigates cases on behalf of his clients which include matters of breach of contract, fraud, and business shareholder disputes.