

***Guest Article:***

**Data Privacy and Artificial Intelligence**

By Dr. Kevin Streff

April 17, 2024

**One cannot open a newspaper, read an online article, or watch the news without seeing something concerning artificial intelligence. AI is mimicking people online. AI is feared to replace employees. As it relates to our financial system, AI is being used to impersonate and commit fraud. Just as we begin to get control of our technologies and IT exams, game changers like AI come along and disrupt it all. Some have suggested banking not being allowed to use AI, while others have advocated that all AI systems and developers must be registered with the federal government. The latest apprehension is that as data privacy threats and laws emerge, AI will exponentially magnify these concerns. Thus, the field of AI privacy is born.**

**AI privacy**is the set of practices and concerns centered around the ethical collection, storage, and usage of personal information by artificial intelligence systems. It addresses the critical need to protect individual data rights and maintain confidentiality as AI algorithms process and learn from vast quantities of personal data. AI fundamentally relies on using large and disparate datasets to draw conclusions that without this technology or data aggregation, would not be possible. The potential is fairly obvious, but equally obvious is that if this is not managed well, unintended consequences are sure. And in the banking sector where data privacy and artificial intelligence introduce risk to the banking system, it is only a matter of time before the regulators determine what the requirements are and how they are going to enforce them.

What does this all mean for your financial institution? It means accountholders are being impersonated at unprecedented levels. It means data privacy protection moves up the priority list to keep data safe and comply with state and international requirements. It means your vendor management program must be expanded to include data privacy reviews and diligence. It also means you need to build an operational infrastructure to answer accountholder questions about their data, including what data the bank has, where is it stored, and who is it shared with. Privacy policies and notices are required to provide directions on how privacy practices will occur at your bank. It means that your bank needs to get ready to be asked risk-based questions about data privacy, including what your bank is doing to control data privacy risks.

What should your bank do? Two obvious things come to mind. First, name a Privacy Officer. This reminds me of 20 years ago when information security first began to rear its head, and one of the first things banks did was name a Security Officer. The examiners like that someone was in charge and trained in on the topic. The new Privacy Officer could be an expended role for your current Information Security Officer, someone in marketing or legal, or a management employee in operations. Second, determine a data privacy plan and budget. How? I am currently offering a free gap analysis that takes approximately two hours to assess your environment and build a 3-year plan. The good news is that most of the data privacy actions banks need to take right now do not cost a lot, but how do you know where to start, what to do, and in what order to do them? The gap analysis is one tool to build this data privacy roadmap and demonstrate to bank regulators that you have this issue managed (the M in the CAMELS rating).