

**Do Banks Need Privacy?**

By Dr. Kevin Streff

January 3, 2024

What if the federal government wants to understand if the United States banking system is being used to distribute a new ransomware variant? What if it secretly uses its systems and the core processing platforms to confirm or deny this allegation. The need is real: protect citizens from harmful cyber-attacks. However, what about your privacy? What about the privacy of your data? Where does this balance come in between a party (i.e., government, business partner, vendor, etc.) using or misusing bank and/or customer data?

This is precisely the type of data privacy concern that digital banking is creating: on one hand customers are demanding a bank-from-anywhere platform, but on the other hand they are uncomfortable not controlling and having visibility to how, where, and when their data is being used. International laws in eighteen countries now address this balance, keeping data ownership with the customer and requiring companies to work with the data in only a variety of ways. A dozen states also have data privacy laws that lay down specific data collection and handling requirements, setting up an authority to police actions so that their citizens’ data is handled in accordance with these new requirements. In some of the laws, organizations can be fined 4% of revenue if found out of compliance with the law! These data privacy laws have teeth. In fact, the Consumer Finance Protection Bureau (CFPB) has begun the process of looking for violations and responding to customer complaints with the new state laws. Multimillion dollar fines have already been levied, and this process is just beginning.

It is likely that over the next couple of years a national law is passed outlining United States requirements. Asia, Europe, Canada, and India already have comprehensive laws, yet the U.S. does not. The patchwork of state laws will prove more difficult to manage than a thin federal law that gets to basic data privacy protection requirements. However, in the meantime, banks are left trying to figure out which laws apply to them, what is considered reasonable commercial data privacy protection, and how to get started with an information privacy program (IPP).

Twenty years ago, banks were faced with a similar dilemma: data security. The Gramm-Leach-Bliley Act was passed, banks and regulators alike did not know what an information security program (ISP) or a risk assessment was but were now mandated to invest in these systems. They needed to get the board up to speed on the issue, establish committees to manage the issue, train their employees and customers on risks and best practices, and regularly test and verify their systems for data security issues. Similar requirements are sure to follow for data privacy.

So, what should you do? Get the board and management team up to speed on what data privacy is, what the current laws look like and require, understand what information privacy program options are available, figure out how to conduct a data privacy risk assessment, and put someone at your bank in charge of data privacy (i.e., Data Privacy Officer). Addressing data privacy starts with education: board, management, employees, and customers. Creating an educational program is first and foremost to get everyone on the same page on what data privacy responsibilities the bank has and what it needs to do to address this growing threat.