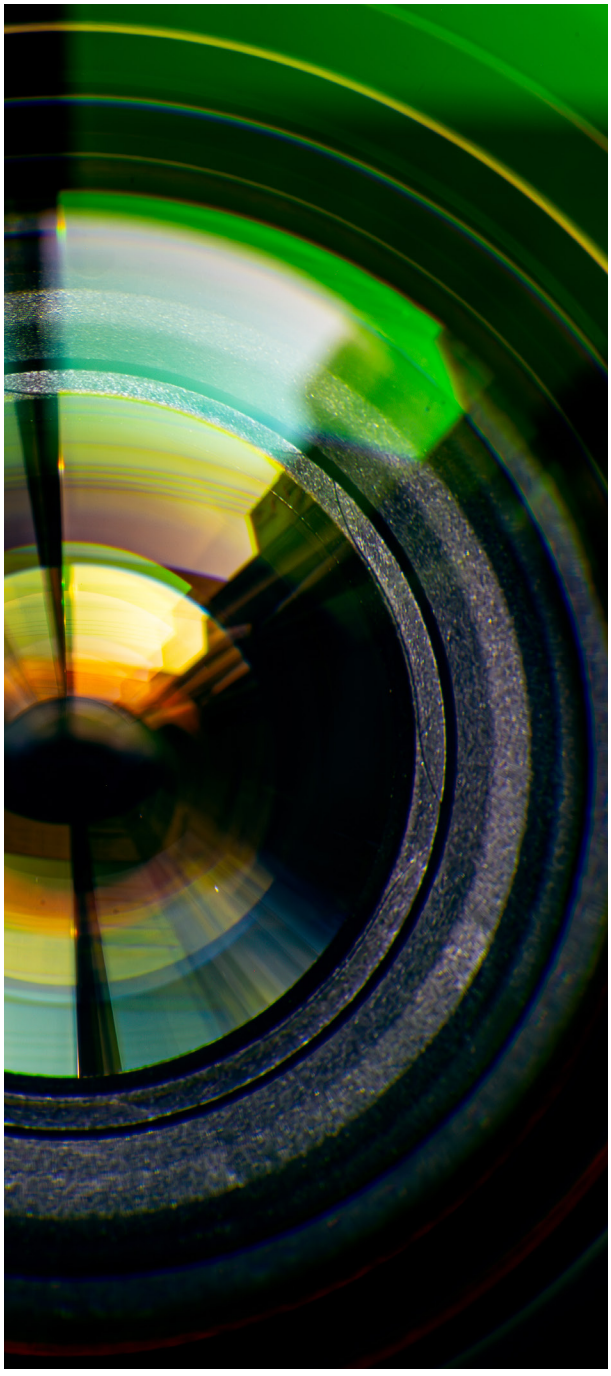
Managing Post-Quantum Data Privacy and Security Issues at the Leadership Level

Written by Liisa M. Thomas



Introduction

Quantum computing is on the near horizon. While leaders may have begun to prepare for the increase in computing capacity, many are not considering the very real – and very significant – privacy and data security law issues. Quantum capabilities will change how businesses need to think about a host of legal issues in this space. Whether it is the potential to reidentify previously anonymous data, the creation of massive datasets to protect, or the threat to today's encryption and identity systems, there are decisions to be made. And the decisions made today will be the story told tomorrow to regulators, boards and courts.

For senior leaders each privacy and security risk brings in three core questions. What, factually, is likely to occur? What are the legal risks and obligations? And how can those risks be mitigated? Companies need more than a checklist to prepare. They need a well thought-through, governance-driven quantum readiness strategy. And to be effective, the strategy needs to be predicated not only on legal requirements and risks, but tenets of organizational change and behavioral science. In particular, one that creates the kind of effective compliance solution that is contemplated by regulators and governmental authorities like the Department of Justice as outlined in its Sentencing Guidelines for the Evaluation of Corporate Compliance Programs. Below is what that path can look like for each risk area.

1. Data Analytics

Quantum computing opens the possibility of large-scale data analytics by those who may have never engaged in any analysis before. Imagine being able to review the full scope and breadth of consumer information you maintain whether in structured or unstructured format. Already, business teams want to maintain data *ad infinitum*, arguing they may "need it in the future!" Realistically, lawyers and data security professionals have argued, you may never use that data. So better to minimize risks and delete. That argument will hold less water in the quantum age. Teams may thus feel the pressure to collect and retain more data. Including sensitive elements like behavioral or biometric data.

If that happens, what are the legal restrictions and risks? Many jurisdictions have data minimization obligations in place. Namely, collecting only that information that is needed for supporting the purpose for which it was originally collected. And relatedly, avoiding "secondary" or supplemental uses. Many also have restrictions in place for processing sensitive information, or restrictions for profiling or certain uses of "automated decisionmaking" technologies. For sensitive information, obligations might include opt-outs/opt-ins, or conducting risk assessments. With regard to profiling, in particular, that which could result in a "high risk" impact on individuals. Things like not getting a job, being denied financing, and the like. Even in locations without these restrictions, housing large datasets can create data security issues.

Typically, companies have attempted to minimize risks by either avoiding the regulated activities (profiling, collection of sensitive data, etc.) *or* by limiting what information is collected. But what can be done in the coming quantum age, in light of business pressures to both engage in these activities and maintain large datasets? Those who have avoided deploying risk assessments, conducting data mapping, or updating vendor contracts will need to have this on their roadmap. Also on the roadmap is a thoughtful compliance program. In this kind of a dynamic environment, that means meeting the business teams where they are at, to avoid an aspirational policy that may contain legal guardrails, but is not followed by any business teams. Organizational change theories tell us this could look like high-visibility champions, or key stakeholders involved early in the process who help develop a system that embeds privacy and security protective approaches.

2. Gaps in Fairness and Transparency

Related to the increase in analytics power is the possibility of creating more detailed inferences about people. In the privacy world, this could fall into "profiling." And, under many privacy regimes, there are heightened obligations – as well as some prohibitions – when engaging in this practice. This is especially true if the profiling ties into automated decisionmaking, where the power of quantum might be paired with generative AI making decisions that result in a high-risk outcome to an individual. Think, not getting a job, medical recommendations, and the like.

Many privacy enforcements are premised on theories of deception. They use as "hooks" portions of privacy laws that require transparency. In other words, explain to individuals what you are doing; i.e., transparency. And if you do not do what you said, that is a deceptive practice. In the world of high-risk, automated decisionmaking, privacy laws do have this transparency obligation. Tell people how you made the decision. That is a problem if a company used a powerful, quantum-based model where it does not have visibility into the decisionmaking process.

In addition to deception-based enforcement, privacy cases are also brought alleging unfairness. Again, privacy laws have codified this, including in the high-risk, automated decisionmaking realm. For example, by requiring human oversight for certain types of decisions. Again, human oversight for a high-powered, quantum based decision will be difficult, if not impossible, given the potential lack of visibility into how the system operated.

Organizations already have an opportunity to begin developing processes to address these risks, as they look to current tools that incorporate generative AI. Flexing the muscle now of oversight will help future-proof. Processes would include documenting how key decisions are made and integrating human review.

3. Anonymous No Longer Anonymous: Reidentification Power

With the power of quantum, companies will be able to more easily reidentify data that is currently anonymous. And their downstream partners, with whom they share "anonymous" information, will as well. Under privacy laws, this will mean data that was originally considered *not* personal information may, in fact, become personal information. Why? Because in many jurisdictions, if data can be linked back to an individual, the law considers it personal data.

If this becomes true, companies will need to tread cautiously. For example, currently many companies give anonymous data to vendors. They rest easy knowing that the information is not personal because the vendors cannot reidentify it. And therefore, privacy laws do not apply. In the future, if that data can "easily" be reidentified using the power of quantum by the vendor, the data could be viewed as personal. These are potentially uncharted waters for both companies – and regulators. Contracts, privacy notices, and data-sharing agreements built on anonymization claims may no longer hold.

There can also be impacts if the company does not intend to reidentify data when it anonymizes it. Then, later, new personnel or different personnel decide that they do want to reidentify the information. Thus what started as a data set outside of privacy law purview becomes a data privacy issue. The datasets will need to be reclassified, and processes put in place to handle the newly personal information. This will have an impact on a variety of the companies' practices. This includes in contracts, external notices – including just-in-time disclosures like those made when seeking consent, and in privacy policies. Not all datasets may be at risk of reidentification, and a tiered, risk-based approach for preparation may be appropriate. How to identify the riskiest datasets? Consider a "premortem" analyzing worst-case scenarios if currently anonymous datasets were to be reidentified. When working with business teams, consider framing the review as a way to protect those programs from future regulatory challenges, rather than a reason to shut them down.

4. Devaluation of Encryption Keys

Encryption has become a ubiquitous way to protect data. The concept, making data unreadable to anyone who does not have the right key, is great. For it to function, the underlying math needs to be too complex for anyone – or anything – to break it. Will this continue to work in a quantum age, when computing power is exponentially stronger and faster? What we are beginning to learn is . . . likely not. A sufficiently powerful quantum computer could break the encryption methods most widely used today. Methods that currently protect a significant share of internet traffic and internal systems.

Right now, many data security laws require encryption. Similarly, many data breach notification laws exempt from a duty to notify encrypted data. The presumption, of course, being that encrypted data is safe from threat actors. This may change with quantum. With quantum on the horizon, organizations should take steps now, if they have not done so already, to explore new security mechanisms. Failing to do so could potentially risk the need to answer questions about whether practices remained reasonable as that risk became more widely understood.

A practical roadmap might begin with inventorying key systems, and migrating to encryption methods that are resistant to quantum attacks. The National Institute of Standards and Technology has recommended a set of such methods.

5. Mass Harvesting

A final word of caution. Threat actors may be amassing large datasets of encrypted information, with the hopes of using quantum in the future to decrypt that information. Databases, communications, and files that are protected by today's encryption could be exposed in the future — even if no breach occurs now. Companies that face breaches of encrypted data where there would not otherwise be a duty to notify may, understandably, be concerned. Particular consideration may need to be taken for acquired datasets that contained sensitive data.

When developing protection measures, factor this risk into data retention schedules. For sensitive data, is it truly needed for as long as it is currently being kept? What additional security measures could be put in place? How have vendors' retention and protection measures been analyzed? Starting this work with a focused review of the data the organization holds that has the longest confidentiality requirements can serve as a manageable starting point. Involving business, legal, and risk teams in that review early could produce more lasting results.

Conclusion

Quantum risk is often framed as a purely technical puzzle, but the hardest problems are not about algorithms—they are about people, process and accountability. The choices companies make today about how much data to collect, how long to keep it, how to monetize "de-identified" datasets and how quickly to prepare for post-quantum cryptography will impact their future risks. They will also shape how regulators, customers and business partners judge whether the company took "reasonable" steps in the face of a widely discussed, foreseeable shift in the threat landscape.

Organizations that will be best positioned use the quantum moment as a catalyst: to tighten privacy governance, modernize security architecture and embed crypto-agility and change-readiness into their culture. That work is inherently cross-functional and benefits from tested frameworks, scenario planning and practical change tactics that anticipate internal resistance, not just technical roadmaps.

Contact

Liisa Thomas
Partner • Co-Leader, Privacy and Cybersecurity Practice Group
+1.312.499.6335 • Chicago
lmthomas@sheppard.com