NAVIGATING THE RISKS OF PROCESSING EMPLOYEE-GENERATED DATA

F. MARSHALL WALL
CRANFILL SUMNER & HARZOG, LLP

Although the use and abuse of user-generated data by social media companies has dominated national headlines for years, privacy advocates have started raising concerns in response to the increasing collection and processing of employee-generated data in the workplace. In recent years, many employers have gone beyond the traditional forms of monitoring for the sake of policy enforcement and trade secret protection and have started to consider how they can use advanced data analytics in support of various organizational goals and priorities.

While it is easy to wonder if implementing an internal data processing initiative is right for your organization, it is important to be aware of the various risks that come with transitioning from a monitoring policy to a processing policy. By way of example, the International Association of Privacy Professionals (IAPP) recognizes four general categories of risk that an organization should contemplate and address prior to implementing a data collection and processing policy: legal risks, reputational risks, operational risks, and investment risks.[1] While the reputational, operational, and investment risks of a data processing initiative are subjective, the legal risks are more objective and concrete. While this article is not intended to be an exhaustive review of employee workplace privacy, it will help demonstrate the need for having a well thought out information management plan prior to initiating a data-processing operation at your own organization

International Law

Although the General Data Protection Regulation (GDPR) is a European Union (EU) regulation, it is applicable to many US companies. The GDPR provides data privacy protections for EU citizens both domestically and abroad. Accordingly, the language of the GDPR covers a variety of data-processing activities on a potentially global scale. By way of example, the GDPR covers companies engaged in data processing in the EU as well as companies that offer goods or services to (or monitors the behavior of) EU residents. It can also apply to companies that process and hold the personal data of EU residents, regardless of the company's location or business activities.

Although the GDPR has been in effect for a little over a year, many US companies are still unsure of the various ways it may affect their business operations moving forward. Based on the broad scope of activities and individuals, the GDPR can impact North Carolina businesses in a variety of ways that can feel confusing and difficult to understand. This issue is further complicated by the unexpected costs that can arise when processing data compliant with the GDPR. Among other things, the GDPR provides the data subject certain rights of access, portability, and breach notifications that can become costly and time consuming to implement. The GDPR also threatens steep penalties for compliance issues up to a maximum of 4% of annual global "turnover" or 20 million euros (whichever is greater) for the most serious infringements.

Accordingly, it is important to consult with a data privacy professional in order to understand the potential impact the GDPR could have on your business' efforts to process employee data. Although the GDPR obligations can appear onerous and difficult to understand, a trained privacy professional can help your organization navigate the GDPR and reap the benefits of internal data processing activities.

Federal/State Law

In contrast to the EU, the US does not currently have a Federal law analogous to the GDPR. However, there are many situations where various state and Federal regulations touch on, and potentially restrict the use of, employee data. Under the current US system, the applicability of any given regulation largely turns on the type of information that is being collected, and the purpose for which that information is going to be used. Understanding the US system can be further complicated by the variety of government agencies that are responsible for enforcing this patchwork system. While some regulations may be enforced by the Department of Labor, others can be enforced by the Federal Trade Commission (FTC) or the Consumer Financial Protection Bureau (CFPB).

Both North Carolina and Federal law provide certain protections over a range of information that an employee may possibly pass along to their employer, such as protected health information, Social Security numbers, and bank account information. Consequently, your organization should speak with employment and privacy professionals to discuss what information you intend to use and how you intend to use it. Although each organization's needs and concerns will differ, there are some laws that will apply to most organizations collection and processing efforts.

At the Federal level, there are three major regulations that address the collection and retention of workplace communications: the Wiretap Act, the Electronic Communications Privacy Act (ECPA), and the Stored Communications Act (SCA). As most employers are already engaged in some form of employee communications monitoring, it is important to understand how these laws may impact your data processing initiative.

As a general matter, the Wiretap Act and ECPA provide strict restrictions on the interception of wire communications, oral communications, and electronic communications. Accordingly, these laws cover phone calls, emails, and other electronic communications. However, most employers that engage in some form of interception based monitoring fall into one of two exceptions provided under the laws. Generally, the employer has either obtained the consent of one of the individuals that is party to the communication, or the interception was done "in the ordinary course of business."

Similarly, the SCA generally prohibits unauthorized access to electronic communications while it is in a facility through which an electronic communications is provided. However, the law also provides some carve-outs for an employer that either is the entity that provided the services or is the user of the service with respect to a communication of, or intended for the company. North Carolina also has several pieces of legislation that mirror the workplace employee privacy protections offered by Federal law. By way of example, North Carolina generally prohibits the installation or use of a pen register or "trap and trace" device without first obtaining a court order. However, there are certain exceptions whereby the installation or use is permitted, such as with the user's consent.

Despite the potential safe harbor, there are a variety of ways in which an employer may unintentionally run afoul of these restrictions. For example, an employee may have signed a consent release that covers various forms of employer monitoring. However, an employer should be wary of relying on prior consents to expand collection and monitoring procedures without engaging in a thorough review of the activities and purpose of the data collection activities contemplated in the release. Violations of these laws can carry criminal charges and private rights of action.

Ultimately, it is important that your business carefully contemplate the various risks associated with collection, retaining, and processing employee-generated data. While the potential benefits of such an initiative may be high, the penalties for misuse are higher. Consequently, spending time implementing a well designed data management policy can help your company minimize risks while maximizing returns.

[1]Swire, Peter P., and DeBrae Kennedy-Mayo. *U.S. Private-Sector Privacy: Law and Practice for Information Privacy Professionals.* International Association of Privacy Professionals, 2018

CRANFILL SUMNER & HARTZOG LLP

F Marshall Wall

F. Marshall Wall is Managing Partner at Cranfill Sumner & Harzog LLP. Wall represents clients in a wide range of disputes encompassing business issues and commercial litigation. He serves as Chair of the CSH Law Liability & Privacy Law Practice and holds the Certified Information Privacy Professional/United States (CIPP/US) designation. He is also board certified by the North Carolina State Bar as a specialist in Privacy and Information Security. He was part of the first class of attorneys in North Carolina to be certified in this area of the law.CSH Law Associate James King assisted in preparing this article.