GT GreenbergTraurig

Ten Privacy and Data Security Mistakes Start-Ups Should Avoid

– Françoise Gilbert | gilbertf@gtlaw.com | 650.804.1235

Most technology start-up companies lack the experience and resources needed to manage the plethora of security, privacy, and compliance issues inherent in a growing technology business. Nevertheless, the legal and business implications of poorly managed privacy and data security practices are too important to ignore. A single error can undermine the trust of investors and customers, attract unwanted regulatory attention or litigation, and ultimately, derail a start-up's success. Here are 10 common privacy and data security mistakes that start-ups must avoid.

1. Assuming privacy or security is just for the geeks

Too frequently, company management and boards fail to pay sufficient attention to the significant problems that will arise from a company's failure to provide adequate security or to comply with applicable privacy laws. Litigation involving privacy and security is now mainstream.

In addition, there is a rising number of shareholder derivative actions for breach of fiduciary duty stemming from failure to supervise the company's activities related to privacy and security, such as lack of compliance or failure to meet commonly used practices. For example, they could be initiated by a disgruntled minority investor who is concerned that his investment has not been managed with proper care.

2. Ignoring relevant rules and laws

Some tech start-ups may pay little attention to the fact that businesses are governed by a wide range of laws and standards, and are expected to operate within commonly accepted practices. Among other things, they may ignore that the collection, use, and processing of most personal information in the United States and abroad is regulated. Ignoring these laws may lead to significant errors and trouble.

Among other things, ignoring privacy or security obligations may come to haunt a start-up when it meets its first major customer or business partner. It may receive a superb offer for a contract with a large company that does require certain assurances of compliance with applicable laws. The start-up will be expected to have in place the same levels of protection, awareness, or maturity as its larger client. If it does not have the proper structure in place for its operations to be compliant with applicable laws, it will struggle to meet that client's expectations, and may have to create in three months what it should have built over three years. If it cannot meet the client's standards, it will not be able to sign a contract.

3. Thinking that they are flying under the radar

Start-up tech companies may elect to ignore their legal obligations because they are small and can easily fly under the radar. They might be able to fly under the radar for a short time, but not for long.

Litigants and enforcers are not particularly sympathetic to a defense based on the size of a company. They are more focused on the actual effect that the mistake, abuse, security incident, or legal violation may have on the public at large. If they determine that the effect is significant, the fact that it was caused by a five-person company is likely to be irrelevant.

4. Ignoring the benefits from processes and policies

Start-ups may think that their ability to succeed require that they be nimble. They may believe that policies and processes slow them down and are not for them.

In the absence of rules defining who is allowed to access certain information or what uses are restricted, employees, subcontractors or visitors might inadvertently access highly confidential or sensitive data and misuse it. Policies and procedures provide a frame of reference and guidelines that show how to proceed, and help make decisions faster. When properly applied, they can increase efficiency and reduce errors because they help build harmony and unity of actions around the company's goals.

5. Believing that they are not responsible

Many tech start-ups hire third parties, outsource some functions, or locate operations in the cloud, because they do not have sufficient resources to hire personnel or to purchase equipment. In doing so, they may think they have passed on to those third parties the responsibility for their data. However, the company that initially collects the data remains primarily responsible for anything that happens to the data. The entity that the customers know – not the obscure service provider – will be the one that will be sued or investigated if data is illegally processed or inadequately protected. It will be the one whose reputation and trustworthiness will be most at risk.

6. Failure to provide adequate security

Many US states and foreign countries require that companies provide adequate protection for the data – or certain categories of data – in their custody. A company's size is not an excuse for failing to seek the proper resources, technologies or experts to ensure the adequate level of security adapted to the nature of the data stored or processed by an entity.

Security breaches are to be avoided by all means. They are significantly disruptive. A company that has implemented a thought through written security program will be less exposed to potential security breaches and to the significant consequences of security breaches. In most cases, a company that has suffered a breach of security might be required to publicly disclose the occurrence of the breach. It may have to send notices to affected parties and regulators, and offer credit monitoring or identity theft insurance, which is usually a significant expense. If a state or federal regulator becomes aware of the breach, a lengthy and grueling investigation of the company's practices may follow, resulting in significant cost, disruptions, and potentially ending with an order that submits the company to the supervision of that regulator for the next 20 years.

7. Assuming that bigger is better

Some tech start-ups tend to collect much too much data just because "we may need it later" and "storage is cheap." The more data a company has in its custody, the more vulnerable it is to legal violations and security breaches.

Collecting too much data can cause a compliance issue; some laws require entities to collect only the minimum amount of data necessary to achieve a stated purpose. Additionally, having a lot of data can become a significant charge. For example, some laws grant individuals the right of access to data that a company holds about them. In case of an individual's request for access to data, the company will be required to provide copies of files that may be located in different locations, on different devices, or in different formats. The more data a company has, the more time and data experts it will need to retrieve it. Collecting a massive amount of data also causes significant security risk. The larger the volume of data the higher the probability that it will be stolen.

8. Copying the privacy policy of the business next door

Start-ups often hope to "save" on legal costs by simply copying the privacy policy of another website without fully understanding what it means, or ensuring that the document describes accurately the start-up's policies and procedures. The borrowed document is likely to tell a story other than that of your company. It will describe the neighbor's practices, which may be significantly different from those of your company, or, worse, may be illegal. From a legal standpoint, this may end up constituting misrepresentation, which can be prosecuted by a state Attorney General and the Federal Trade Commission and in some states by competitors for "unfair or deceptive practices."

If you were to run a marathon, would you borrow your neighbor's shoes? No. You would be concerned that they would not fit you. You would fear that you could be hurt and unable to continue for the entire distance. Similarly, a borrowed privacy statement likely will not fit your company and may significantly hurt you in your race to the customer. It will not reflect your company, its values, its practices, or its objectives. It may state commitments other than those you would want to make.

9. Making representations that they don't understand

It is true that legal documents may be long or difficult to read. That is not an excuse for not reading them with a critical eye. Privacy statements of some tech start-ups state "we will never sell your personal data." This might be their intention at a particular time, but it fails to take into account that the company or a portion of its assets might be sold. An asset deal may be blocked because the main asset of the company is its database, and per the statement in the privacy policy, the database of personal data cannot be sold.

10. Misunderstanding the effect of anonymization

When discussing personal data protection, it is common to hear: "We don't have any personal data, our data is anonymized, and it cannot be tied to an individual." This is a significant mistake. While it might have been true, a long time ago, that anonymization prevented the association of a particular individual to a particular data set, this is no longer the case. In the world of data analytics, big data, semantics and other tools, there is no such thing as anonymity. Too often, a competent data scientist will be able to crack the anonymization shell in a short time.

Be proactive from the start

It is clear that technology start-ups need to be proactive about privacy and data security from a very early stage. Small size and limited means are not valid excuses.

- Pay attention to your practices and procedures when handling personal data and sensitive business data.
- Take the time to build and maintain a data map that identifies what data is expected to be collected and from whom, and how the data is expected to be used, stored, transferred and destroyed.
- Design a data privacy and security program that addresses your company's compliance obligations and ensures adequate data protection.
- Translate this program into clear and accurate public disclosures about your company's practices.
- Periodically revise the program to take into account the developments in the company and its business.
- Train your staff, employees and independent contractors, so that they understand their obligations.
- Do not procrastinate and wait for the day when you need to respond to a due diligence questionnaire.