Human Rights for Small and Medium Sized Technology Companies: Privacy and Data Protection

June 2020

GLOBAL PARTNERS DIGITAL

OPEN TECHNOLOGY INSTITUTE

If you are a company that collects data on customers and/or other users, it is important that you develop a set of data protection and privacy policies and procedures. This data could include contact or biographical information like names and addresses, banking information used for payments or financial transactions, content of messages or other information stored on a platform, metadata about the timing and duration of use, location data like GPS coordinates, or biometric information like heart rate or fingerprints. All of this data is sensitive, and sharing it willingly with third parties, or unwillingly through hacks or data breaches, could have serious impacts on the privacy of those users.

Threats to individual privacy and security are only growing, as we have seen with major data breaches and scandals occuring in the technology industry over the past few years. Governments may also approach companies seeking data they have collected on users, using legal tools like warrants to compel companies to provide that information to law enforcement. All of these scenarios pose complicated privacy challenges, and rigorous policies for protecting user data are important for any company that collects and processes it. We recognize that smaller companies are often constrained in terms of resources and personnel. Here are six important best practices for developing data protection policies and processes:

Essential

1. **Evaluate your data collection**: Review your company policies and activities to catalogue the different types of data you collect, and from which users. Having a comprehensive understanding of your data profile, as well as the level of risk posed by the information you hold, is important when developing data protection practices.

2. **Minimize the data you collect**: It is a best practice to minimize data collection, and only collect the information your company truly needs to support your products and services. Many organizations collect far more information than they actually need. Data may be valuable to organizations for purposes of research, advertising, and implementation of new features, but much of the information collected isn't necessary for the product or service to function. For example, even though it could enable extra features, location information may not be necessary to maintain an account with your product or service. Organizations should be transparent about what data is being collected and when, and allow users to control the amount of information that is being collected about them.

3. **Minimize the period of data retention**: The more user data retained, the higher risks posed by data collection and storage, such as data breaches and other unauthorized access. It is important to set strict time limits so that your company only holds onto data for the period that it is needed. In addition, your company should disclose to users the timeline for deletion of different types of data like messages, photos, recordings, or accounts, to help users decide what type of information they want to use with the product or service, and allow them to better understand the risks posed by retention of that data.

4. **Be transparent about, and limit the ways data may be used**: It is a best practice that organizations disclose the ways that they may use information that they collect from users so that they can make more informed choices about how they use that product or service. Also, organizations should give users the ability to opt in or out of certain types of data use, like use for targeted advertising, and avoid using data in ways that the users have not consented to. This is good for protecting user security and privacy, as well as maintaining user trust and confidence in a service.

Advanced

5. **Develop and disclose a process for responding to government requests for user data**: Intelligence and law enforcement agencies have long sought data directly from companies, and as many kinds of companies collect and store more data, the number of requests for this data from these agencies has increased. Companies must develop clear policies for processing and responding to government requests. This is a critical but challenging process, and seeking assistance from legal counsel is important if at all possible. It is a best practice to provide notice to users when their data has been requested to the maximum extent permitted by law; however at times the provision of notice can be delayed for ongoing investigations subject to applicable laws. In addition, companies should develop procedures to assess when a government request for data may be unauthorized, inappropriate, overbroad, or otherwise not compliant with legal standards. These procedures should also make clear what steps a company should consider taking when requests meet these criteria, including requesting clarification, complying only in part, or challenging the request. Once a company has established these procedures, they should share at least a high-level overview of these guidelines publicly. The Global Network Initiative Principles on Freedom of Expression and Privacy,[1] together with their more detailed Implementation Guidelines, [2] can help with the design and implementation of such systems and processes.

6. **Implement data security best practices**: There are a variety of best practice tools that can be used to protect users' security and privacy, as well as reducing financial and reputational risk to the company or organization. These may not all be relevant to every company, but some best practices to consider include:

    - *Encrypting data in transit and at rest* to prevent breaches and information theft
    - *Establishing a vulnerability disclosure program* for incentivizing independent security researchers to help identify and report vulnerabilities in software and hardware
    - *Adopting secure authentication practices*—like not using default passwords, requiring passphrases of a certain length and complexity, enabling multi-factor

authentication, and notifying users when account security settings have changed—can help reduce the chances of a breach;

- *Testing products or systems against known exploits* (also known as "penetration testing") to help reduce the chances of a serious vulnerability in your systems
- *Regular patching, ideally with automatic updates*, to ensure that users benefit from the most secure version of the software
- *Implementing breach notification processes* that are publicly available for users to review
- *Developing mitigation processes in case of a data breach* to help increase user trust and prevent further security breaches

Endnotes

1. https://globalnetworkinitiative.org/gni-principles/
2. https://globalnetworkinitiative.org/implementation-guidelines/

GLOBAL PARTNERS DIGITAL

Second Home
68 Hanbury St
London E1 5JL

+44 203 818 3258