DATA ERASURE vs. RISK MANAGEMENT
The Clash of Privacy and Protection of Vulnerable Populations

By Gregory Love, Kimberlee Norris & Georgia McKnight
Date: 4-20-2023

PROTECTING PERSONAL INFORMATION

Everyone has a story about personal information fraudulently obtained by a security breach, Phishing email scam, or sold by a vendor gathering personal information in an online transaction.

Often, consumers knowingly share data with a website, mobile app or web app in exchange for services (i.e., Instagram, Facebook, Twitter); by doing so, the consumer gives the online provider the right to monetize the consumer's data. Too many times, however, entities are engaged in digital tracing where advertisers use the consumer's social media activity, like comments, shares and feelings to profile the consumer and send personalized marketing and media.

The European Union responded with a legislative response empowering individuals; similar efforts are being considered in the United States.

General Data Protection Regulation (GDPR)

In response to consumer outcry in Europe, the EU passed the General Data Protection Regulation ("GDPR") in 2018, the strongest privacy and security law in the world to date. In the age of the Internet and other quickly evolving technologies, this regulation seeks to protect individuals by requiring organizations to safeguard personal data and uphold the privacy rights of any individual residing in EU territory.

To this end, the GDPR protects the *'data subject's privacy rights'* in the EU, granting the individual the 'right to erasure'. In addition to data security requirements and disclosures, the GDPR gives consumers the right to withdraw their consent by requesting that an organization delete all personal identifying information. Data erasure requests must be honored by the organization in possession of the data; failure to comply may trigger significant fines and penalties.

Requests for Data Erasure
Utilizing the GDPR, individuals in the EU are empowered to request and enforce data privacy through the right to erasure, which involves a two-step process: (1) identify all entities in possession of the individual's personal information; and (2) request that the individual's personal information be deleted or erased.

Online applications are available to help individuals accomplish both steps; apps like: Incogni, Mine, DeleteMe, Jumbo Privacy and Just Delete Me. The use of these, and other similar applications, are in widespread use in the European Union, with vendors and businesses required to honor the requests.

Data Erasure in the US
Currently, there is no national GDPR equivalent in the United States. Several states, however, have begun to pass legislation in support of individual privacy. For instance, California passed the California Consumer Privacy Act ("CCPA") in 2020, which gives California residents greater transparency and control over how businesses collect and use their personal information, and includes a *right to delete*. The CCPA appears to be a California equivalent to the GDPR, without the strict penalty provisions.

Similarly, Virginia enacted a comprehensive data protection law, the Consumer Data Protection Act ("CDPA"), which went into effect on January 1, 2023. Several other states, including Colorado, Utah and Connecticut, have passed similar privacy laws going into effect over the course of 2023; expect more states to follow, with the possibility of federal legislation.

The privacy rights of individuals worldwide have been threatened, and lawmakers around the world are reacting, introducing legislation to protect the individual's right to privacy – *including the right to erasure*. As lawmakers craft legislation designed to further privacy rights of the individual, they must balance risk management – *particularly risk to vulnerable populations.*

BALANCING PRIVACY AND RISK MANAGEMENT
Notwithstanding an individual's right to privacy, there are compelling exceptions to an individual's *right to erasure*: one such exception is the need to document abuse prevention efforts. Intrinsically, vulnerable populations are at higher risk of sexual and physical abuse, exploitation, neglect and maltreatment.

Organizations that serve vulnerable populations are under increasing pressure to ensure that these populations are served in safe environments. Vulnerable populations include children and adults (or children) with intellectual or developmental disabilities, or special needs. These individuals are served by schools, camps, churches, mentoring and after-school programs, rehabilitation facilities, ID/DD facilities, youth sport programs and other organizations.

Each of these organizations must *staff* its programs that serve or care for vulnerable populations. The screening process for paid staff and volunteers (collectively "staff members") involves data collection through applications, reference checks, interviews and background checks. Staff members are also required to complete training courses related to abuse awareness, prevention and reporting.

Effective *screening* is an element of organizational *standard of care*: the reasonable and necessary measures taken to reduce the risk of harm to vulnerable populations served by the organization. These measures are required by legislation, licensure, insurance carriers and industry best practices.

It is paramount that organizations take the steps necessary to *meet* standards of care, and equally important to *document* organizational safety measures, preserving this documentation so long as a need exists to demonstrate compliance. Because statutes of limitation for *civil liability* are long and growing longer–and in some states *indefinite*– the need to preserve compliance documentation *cannot* be limited. In short, data related to organizational efforts to screen and train staff members cannot be erased.

Data Erasure Exemptions

Under the GDPR as written, several exemptions would likely apply to organizations serving vulnerable populations when requested to remove personal data. These include exemptions pertaining to 'furtherance of public interest' and data 'used to comply with a legal ruling or obligation.' Without these safe harbors, however, organizations would be required by law to erase information related to the fitness (or lack of fitness) of a staff member to serve vulnerable populations, including criminal histories, incident reports, allegations of abuse, witness statements and more.

The CCPA (California)[1] and the CDPA (Virginia)[2], likewise create data exemptions in matters regulated by laws such as HIPAA[3], GLBA[4], FCRA[5], FERPA[6] and COPPA[7]. The exemptions are broad, but are not focused on the needs of organizations that serve vulnerable populations.

At the same time, state and federal lawmakers are working hard to pass legislation to prevent organizations from 'passing the trash' – allowing teachers, coaches or medical professionals engaged in unethical or abusive behavior from simply moving on to the next place.

It is not hard to imagine how a data erasure request can undermine safety measures if an individual accused of abuse in a mentoring program, for example, makes a data erasure request that all personal information be deleted, then seeks access to children in Program No. 2. When Program No. 2 contacts the prior program for a reference, operative information that might warn Program No. 2 has been *erased.*

Clearly, any iteration of data protection legislation promulgated in the United States must safeguard control of personal data, while taking into account the concurrent risk to organizations serving children and other vulnerable populations. Protect the privacy rights of individuals, *but not at the expense of child safety.*

SUMMARY – THE BALANCE

As support gathers for further data protection regulation, lawmakers must be aware of all interest forming part of the equation. As written, the GDPR carefully curtails the 'right to be forgotten' with exemptions promoting public interest. If similar data erasure rights are considered in the United States, lawmakers must include current exemptions found in the GDPR, carving out a specific exception for organizations serving vulnerable populations.

[1] The California Consumer Privacy Act of 2018
[2] Consumer Data Protection Act of 2023
[3] Health Insurance Portability and Accountability Act of 1996
[4] Gramm-Leach-Bliley Act of 1999
[5] Fair Credit Reporting Act of 1970
[6] Family Educational Rights and Privacy Act of 1974
[7] Children Online Privacy Protection Act of 1998