Worldwide Privacy Regulations Restricting Access to Genealogical Records

Jan Meisels Allen
Chairperson, IAJGS Public Records Access Monitoring Committee
janmallen@att.net

Genealogists need records to do their genealogy. Globally, access to public records is becoming increasingly difficult. There are two main developments limiting access to records by genealogists: the expansion of the "right to be forgotten/erased" which could prevent genealogists from searching their ancestry by names, places or events; or governmental legislation and regulations that lengthen the time during which vital records are not available for public inspection. You need to become engaged in your state/province/country to help retain access to these records that are so important to genealogical and historical research. There is an erroneous opinion by some legislators and regulators that identity theft is caused by genealogists and therefore records access must be restricted—either by time from the date of occurrence and or by relationship. It has been documented that identity theft is caused by large data breeches occurring in financial, government and healthcare organizations, such as the recent Anthem, Equifax, Target, and Yahoo, occurrences.[1]

Privacy is someone's right to keep their personal matters and relationships secret. Accessing genealogical records about living person's conflicts with permitting living persons to retain their privacy. Legally, the dead have no privacy rights. However, governments often embargo death records for any number of years: 0, 25, 50, 100 or more. Who are they protecting? Do they not understand that access to the death record may save lives by being able to trace back genetically-inherited diseases, such as BRACA ll which not only has markers for breast cancer but also prostate cancer and pancreatic cancer? Ashkenazi Jews have a higher propensity for carrying the BRACA ll gene than non-Jews, although those that come down with the diseases with the gene are a very small percentage compared to those without the gene. The European Union's impending General Data Protection Regulation (GDPR) is another instance where privacy and access to records may impede genealogists' access to records—see below.

The International Association of Jewish Genealogical Societies (IAJGS), while understanding the privacy concerns of both the public and governmental agencies, will continue to advocate for access to all records relevant to genealogical research. Individual genealogists should respect requests made by persons asking that certain information about themselves or family members be kept private. (IAJGS Code of Ethics)[2].

The European Union's General Data Protection Regulation (GDPR)

In April 2016, the European Union Parliament approved the General Data Protection Regulation[3]—**it became effective May 25, 2018**. It replaces the Data Protection Directive 95/46/ec as the primary law regulating how companies protect EU citizens' personal data. "It was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy."[4] There are substantial penalties that may be

[1] https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html
[2] http://www.iajgs.org/blog/code-of-conduct/
[3] https://gdpr-info.eu/
[4] https://www.eugdpr.org/

levied for non-compliance by data controllers, organizations, including employers who do not follow the letter of the regulation. Non-compliance includes EU countries that may not adapt their local country laws to be compliant with the EU GDPR prior to the effective date. The GDPR codifies the "right to be forgotten" requiring any company to delete personal information under the right to be forgotten requirements, not just search engines. The provision does **not** apply to deceased individuals. It requires individual countries to provide personal data for archival purposes for holocaust, war crimes, etc. The GDPR also requires consumers to give explicit consent to process their data. Additionally, companies based outside the EU are required to obey the EU laws when offering services in the EU (extraterritoriality).

Personal data transfer between the EU countries and non-EU countries is an issue that has also been very controversial. The long-standing data transfer agreement between the EU and the United States, Safe Harbor, was invalidated by the Court of Justice of the EU (CJEU) in 2015. The replacement data transfer agreement, Privacy Shield, while currently in place, has some in the EU concerned that it does not adequately protect personal data. There are about 2,400 companies that are registered under the Privacy Shield. These include companies that genealogists use, such as DNA and genealogy firms, Google, Facebook, Microsoft and others. The recent enactment in the US of the CLOUD Act requires internet companies to hand over personal data to the U.S. law enforcement agencies no matter where that data is stored.

Right to be Forgotten and Effect on Access to Records Access Globally

While the GDPR does many things, the one issue most important to genealogists is the "right to be forgotten"/"right to be erased". This effectively "erases" history by permitting individuals to have the data controller –such as search engines, employers, etc. erase their personal information such as name, email address and other personal attributes. We have already seen some country archives, and a genetic testing firm, remove data from their websites concerned that it might be in violation of the GDPR[5].

The right to be "delisted" is already law in the European Union due to a 2014 ruling by the CJEU, the highest court in the European Union, establishing this concept and permitting individuals to request articles about them to be removed from search engines, such as Google, Bing, Yahoo and others. Search engines make the determination whether or not to delist if the information is "inaccurate, inadequate, irrelevant or excessive" and whether there is a public interest remaining available in search results. Search engines make their information available in "transparency reports" to let the public know the number of URLs submitted, the number delisted and not delisted. Google is the predominant search engine in the EU and its most recent transparency report states 43 percent of the requested URLs have been delisted out of 2.4 million URLs requested be delisted from 654,800 requests received between May 29, 2014 and February 27, 2018.[6]

Worldwide privacy issues are increasingly becoming prominent—whether it is the worldwide creep of the "right to be forgotten" or government regulation of what a search engine may or may not do. This pits privacy and freedom of speech against each other. In Europe, privacy prevails, while in the US, freedom of speech is part of our Constitutional rights. Those with roots in any of the 28 European Union countries should be concerned with this practice of "erasing history". Countries outside of the EU, such

[5] www.regionaalarchieftilburg.nl/home/blog-detail/algemeen/2018/02/20/gezinskaarten-binnenkort- offline/; http://www.oxfordancestors.com/component/option,com_frontpage/Itemid,

[6] https://transparencyreport.google.com/eu-privacy/overview

as Argentina, Brazil, Hong Kong, Japan, Mexico, Russia and more have either legislatively or by judicial action adopted the "right to be forgotten.

The French Data Privacy Regulator, CNIL, directed Google to delink from all their databases, not just in France—declaring that anywhere in the world, even those websites outside of the EU—were subject to the ruling, upholding a 2015 French Court decision of extraterritoriality. Google offered a compromise based on geolocation of a person's IP address. In March 2016, the CNIL found Google's compromise inadequate and fined Google € 100,000, stating, "the different geographical extensions, i.e. .ca, .com, .es, .fr, .uk etc. are not considered separate treatments but a service adapted to the national language of each country." France's highest administrative court, *Conseil d'Etat* has referred the case to the CJEU asking if their 2014 ruling was to be extraterritorial. We are awaiting the ruling.

Canada and the Right to Be Forgotten

In 2017 the Canadian Supreme Court ruled on a case that made delinking search results extraterritorial—outside of Canada and worldwide. Google appealed to a US Federal Court which granted an injunction that the Canadian Supreme Court ruling is not valid in the United States due to our Constitutional rights of Freedom of the Press and Freedom of Speech.[7]

Earlier this year, Canada's Office of the Privacy Commissioner (OPC) released its draft policy position, *Reputation and Privacy*[8]*.* Their position paper highlights some potential legislative changes and proposes other solutions. These include the right to ask search engines to de-index web pages that contain inaccurate, incomplete or outdated information; and removal of amendment of information at the source. Both de-indexing and source takedown are included in The Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's law relating to data privacy. The paper defines de-indexing as "the process by which a webpage, image or other online resource is removed from search engine results when an individual's name is entered as the search term. The final policy determination is not yet known.

United States Right to Be Forgotten AND Impediments to Records Access

Despite our Constitutional rights of Freedom of Speech and Press, there are several attempts to adopt "right to be forgotten" in the United States.

California CA 2182 would create a new California regulatory agency, the California Data Protection Authority (CDPA) to regulate Californians' personal data on the internet. All technology companies that serve Californians on the internet would be regulated by the new agency. The bill has been amended to ensure that personal information can be removed from an edge provider's database The edge provider is defined as any individual or entity in California that provides any content, application or service over the Internet and any individual or entity in California that provides a device used for accessing any content, application, or service over the Internet, when the user chooses not to continue to be a customer of that edge provider.

Also, the California Supreme Court is considering a case brought by a lawyer about whom derogatory remarks were posted on Yelp. Defendant was the poster. A default injunction ordered the poster to remove the comments. The poster did not remove them. The lawyer now seeks to force Yelp, a nonparty, to remove the content in question. US Law, Section 230 of the U.S. Communications Decency Act provides for online free speech. Yelp does not face liability as a speaker of publisher of third-party

[7] http://fortune.com/2017/11/03/google-canada-censorship/
[8] https://tinyurl.com/y6whn9n9

speech. If the lower court ruling stands, it creates a de facto right to be forgotten in the United States that could force websites to remove all sorts of content.[9]

New York Last year a bill was introduced in the NY Assembly, A 5323, that would establish the right to be forgotten, allowing individuals to request removal of materials and search engine links when the information that is "inadequate, irrelevant, no longer relevant or excessive". That bill is still in committee.

The New York City Department of Health and Mental Hygiene (NYCDoH&MH), despite over 5,000 comments to the contrary, adopted a regulation imposing excessive embargo dates for when they transfer records to the Department of Records and Information Services (DORIS): 125 years for birth and 75 years for death.[10] Existing records at DORIS are not affected.

As a result of the 5,000 plus negative comments about the extended embargo periods for birth and death records, the NYCDoH&MH proposed another regulation which would expand the family members which could access birth and death records of deceased individuals without waiting for the embargo periods. While this was a positive move, additional family members, such as step-children and step-parents and researchers are desired to be added. The result of this proposed rule will be discussed during the session.

Model State Vital Statistics Act

The responsibility for the collection, registration and reporting of vital statistics (records for births, deaths, fetal deaths, marriages, divorces and annulments) in the United States is vested in the 50 states plus 7 jurisdictions for a total of 57 public health jurisdictions.

The Model Act currently restricts access to birth records for 100 years and restricts access to death, marriage, and divorce records for 50 years. In May 2011, a working group consisting of state and local vital statistics executives issued a final draft of revisions to the Model Vital Statistics Act, which would extend the restriction periods to 125 years after the date of a live birth, 75 years after the date of death, and 100 years after the date of marriage or divorce. The National Association for Public Health Statistics and Information Systems (NAPHSIS) endorsed the Model Act in June 2011. The US Government has never adopted the revised Model Vital Records Act.

It is critical to contact us if you learn if either through legislation or regulation the Model Vital Records Act is being introduced in your state. We have been successful in defeating the attempt to enact the Model Act in several states.

IAJGS Records Access Alert

IAJGS provides an announcement list on records access issues. Depending on what activity there may be, postings may occur several times a day, or not for several days. It is the best way to stay informed of records access activities around the globe. Registration is required. To register for the IAJGS Records Access Alert go to: http://lists.iajgs.org/mailman/listinfo/records-access-alerts. Archives are accessible at: (you must be registered to access): http://lists.iajgs.org/mailman/private/records-access-alerts

[9] http://reason.com/blog/2016/09/22/yelp-refusing-to-remove-reviews-ruled-de
[10] http://www1.nyc.gov/assets/doh/downloads/pdf/notice/2018/noa-amend-article207.pdf