Records Access and Privacy: At a Crossroads

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. Whether it is due to the expansion of the "right to be forgotten/erased" which could prevent genealogists from searching their ancestry by names, places or events; or by governmental legislation and regulations that impinge upon our access to vital records, our access to genealogically relevant records is being challenged. You need to become engaged in your state/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.

Privacy is someone's right to keep their personal matters and relationships secret. There is an inherent conflict between being able to access genealogical records and also permitting a living person to retain their privacy. Legally, the dead have no privacy rights. However, governments 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.

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).

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

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 (EU) countries should be concerned with this practice of "erasing history". In the Spring of 2014, the Court of Justice of the EU (CJEU) declared residents of the EU had the "right to be forgotten" when they decided that a Spaniard who had once been declared bankrupt was entitled to have links to reports of his financial difficulties hidden from anyone who searched his name on Google. This declaration applies to all search engines, not just Google, which has the largest market share in Europe.

While Google has "delinked" about 43 percent of the requested links since May 2014 (as of February 2017)[1], 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. For example, if a German resident asks Google to delist a link popping up under searches for his or her name, the link will not be visible on any

version of Google's website, including Google.com, when the search engine is accessed from Germany. However, the requested "delinked" site would be visible from other countries in the EU-such as France or the United Kingdom. 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." We are still awaiting the decision of Google's appeal to France's highest administrative court, *Conseil d'Etat*. The French Data Privacy Regulator is also the president of the Article 29 Working Group—the group of EU Countries' data privacy regulators.

Countries outside of the EU, such as Argentina, Brazil, Hong Kong, Japan, Mexico, Russia and more countries have either legislatively or by judicial action adopted the "right to be forgotten." We are also awaiting the Canadian Supreme Court's decision on a case regarding extraterritoriality. The Japanese Supreme Court found search results are a form of free speech, even though they are machine – generated and restricting results could be seen as a restriction on speech. Brazil's Supreme Court opined unanimously that the right to be forgotten may not be imposed on search engines. In the United States, a bill establishing the right to be forgotten was introduced in the New York State Legislature. While the Senate version was "pulled" by the author, the Assembly version is still sitting in committee, despite strong opposition as it is in violation of First Amendment rights.

General Data Protection Regulation

For the past five years, the EU has been working on an updated draft General Data Protection Regulation (GDPR). The trialogue - the EU Council, Parliament and Commission, reached a political agreement in December 2015. In April 2016, both the Council and the Parliament formally adopted the GDPR. From its original introduction in 2012 to what was approved in April 2016, the GDPR had 3,999 amendments, more than any other piece of legislation in the history of the EU Parliament.[2] The GDPR will become effective and implemented May 25, 2018, two years after its passage, providing each of the 28-member countries' time to amend their country's legislation to comply with the new EU regulation. The GDPR codifies the "right to be forgotten" requiring any company to delete personal information, not just search engines. The provision does not apply to deceased individuals and requires individual states (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).

Data Transfer between the US and the EU

In 2015, the Court of Justice of the European Union (CJEU) invalidated a 15-year "safe harbor" international agreement permitting digital data transfer between the US and the EU. In a case against Facebook, the court found the data transfer agreement violates the privacy rights of Europeans by exposing them to allegedly indiscriminate surveillance by the U.S. government. The dissolution affects over 4,000 businesses, including genealogical and DNA firms as well as Google and Facebook, which collect and mine data from European users and send it to their home bases in the United States, thus sharing data on EU residents. On July 12, 2016, a new agreement was adopted, known as the "Data Shield" between the EU Commission and the United States. Some in the EU are still concerned that the "Privacy Shield" will not meet the EU privacy requirements.

Federal Communications Commission Rule on Customer Privacy of Broadband and Other Telecommunications Services

In November 2016, the (US) Federal Communications Commission adopted a rule to protect consumer privacy with broadband and other telecommunication services. The FCC required these providers to get prior permission from subscribers to collect and share data on their web browsing, app use, location and financial information. In March 2017, the new Congress passed a joint resolution providing disapproval of the FCC rule. The joint resolution was signed into law by President Trump in April.

Clearly there are titanic differences between Europe and the United States regarding consumer privacy issues.

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, the City of New York, the District of Columbia, Puerto Rico, American Samoa, Guam, the Northern Mariana Islands, and the Virgin Islands.

The Model State Vital Statistics Act (Model Act) was developed to serve as a model for states and the other jurisdictions in preparing laws and regulations on the collection and publication of vital records, as well as the indices to those records. The first Model Act was developed in 1907 by the Bureau of the Census and has been revised periodically. The last revision of the Model Law and regulations was in 1992.

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. Several vital records officials introduced the 2011 Model Act in their state legislatures. The Department of Health and Human Services (HHS) put the 2011 Revision "on hold" in April 2012. Having not much success in in the legislative arena, NAPHSIS is focusing on the regulatory route to get some, if not all, of their Model Act adopted by the states. According to their website, NAPHSIS has a strategic goal to be the national authority on vital records. According to the Center for Disease Control (CDC) web page on the model act, which hasn't been updated since March 21, 2012, DHHS is still reviewing the proposed revisions. A link to the 1992 Act can be found here: http://www.cdc.gov/nchs/data/misc/mvsact92b.pdf

A link to the proposed 2011 revisions can be found here: http://www.naphsis.org/Documents/FinalMODELLAWSeptember72011.pdf

NAPHSIS maintains a web page with links to those states with online records. https://naphsis-web.sharepoint.com/Pages/USVitalRecordsOfficesOnline.aspx

Some Unusual Access Restrictions

Five years ago, Oklahoma enacted restrictions on access to vital records. It was one of the strangest laws ever enacted, as it required only the named person to be eligible to obtain the vital records. This meant for death records, only the deceased could obtain their own record- not family, nor attorneys or even funeral directors. It was a felony if the state staff provided the record to someone other than the named person on the certificate. Despite multiple attempts to amend the legislation, it remained with this unusual provision until 2016, when a new law was enacted permitting certain categories of people to access the records immediately, such as the named person, parents, legal counsel, and law enforcement individuals. In addition, public access to death records was reduced from 75 years to 50 years. The law also provided for online public indexes for births after 20 years and deaths after 5 years to be available at no cost. The state working cooperatively with the genealogical community opened the indexes six months ahead of schedule.

In 2016, Wisconsin amended their vital records statute deleting the prohibition to the public of uncertified copies of vital records in electronic format for an event occurring before October 1, 1907. Therefore, for events after October 1, 1907, electronic copies are not permitted.

Social Changes Affect Vital Records and Privacy

Recent actions in states reflecting changes in social issues will affect how we enter our genealogical data and its privacy. The New Jersey State Registrar refused to place a woman's name on a child's birth certificate as her mother as the child was born to a surrogate and the ovum had an anonymous donor.[3] In Georgia, a suit has been filed against state employees who refuse to issue a birth certificate because the baby's surname does not match either parent.[4] Transgenders are now being given the right to change the gender they were born with on their birth certificates[5] and California is considering legislation with non-binary as one of the gender options on birth certificates.

PRAMC Record Access Alerts

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.

You will receive an email response that you have to reply to or the subscription will not be finalized. It is required to include your organizational affiliation (genealogy organization, etc.). To access the archives, you also must be registered. The archives are accessible at:
http://lists.iajgs.org/mailman/private/records-access-alerts

---

[1] https://www.google.com/transparencyreport/removals/copyright/?hl=en
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
[3] http://www.legalgenealogist.com/2014/02/14/a-multiplicity-of-parents/
[4] http://www.wjcl.com/article/the-aclu-files-suit-against-ga-officials-who-refuse-to-issue-birth-certificate-based-on-name/9174713
[5] http://www1.nyc.gov/site/doh/about/press/pr2017/pr006-17.page