Restriction of Access to Records Is Increasing Threat to Genealogical Research

by Jan Meisels Allen

"Denied! No access! You have no rights to these documents! The individual has rights; you do not!"

Such responses are what family researchers frequently face today and increasingly will hear in the future when they request records. Fearing increased identity theft and invasions of personal privacy, various governments, including the European Union (EU) and the United States federal and state governments, have been proposing tighter controls over access to data of central concern to genealogists even as the pursuit of genealogy increases in popularity. The genealogical community has organized to counter these proposals. Two genealogy groups monitor activity in the world of record access, the International Association of Jewish Genealogical Societies (IAJGS) Public Records Access Monitoring Committee (PRAMC) and the Records Preservation and Access Committee (RPAC), a stand-alone committee. This article identifies current proposals adverse to genealogical interests, describes attempts by organized genealogy to prevent more stringent restrictions and tells how genealogists who are not content to accept such refusals may help in the effort to block them.

Basic Genealogical Point of View

Genealogists recognize that researching one's family history often is more than merely a hobby. It may be critically important in tracing inherited medical diseases as well as in the reunification of family members long thought lost or never known to have existed. Records access does not simply satisfy intellectual curiosity (although that, too, is a valid reason)—it may save lives. Family history research cannot be done without access to birth, marriage, divorce, death, census, voting and property records and a myriad of other records upon which genealogists depend.

In fact, access to vital records not only is critical for genealogical research, but actually prevents identity theft. For example, since use of a death record proves that a person actually is deceased, the decedent's information could not be used fraudulently by others. Access to vital records by family historians has not been the cause of much-publicized identity theft. The major cause is computer hackers who invade government, business and financial institutions. Unauthorized access by hacking has been well documented in the press.[1] To the author's knowledge, virtually no articles have implicated genealogists as the cause of identity theft.

Pending Governmental Actions

The genealogical world currently is facing three major, potentially adverse governmental proposals, the European Union's Proposed Data Protection Regulation, the United States' 2011 Model Vital Records Act and potential changes in access to the U.S. Social Security Death Index Master File.

European Union Proposed Data Protection Regulation

The European Union (EU) serves its 28-member countries in order to provide a single, unified approach to laws, monetary issues and trade issues. The EU currently is grappling with its data protection regulation, which has not been updated since 1995, recognizing that many changes have occurred on the Internet since the current regulation was adopted.[2] In January 2012, the EU proposed a new Data Protection Regulation which is still being debated.

The decision on what will be included in the final data protection regulation and when a final vote by the full EU Parliament will take place continues to change frequently. At the time this article went to press, the most recent information, as reported by the *New York Times* on October 20, 2013, (http://tinyurl.com/ mk9y5bx) is that German Chancellor Angela Merkel has agreed with British Prime Minister David Cameron to delay the EU Parliament's vote perhaps as late as sometime in 2015—after the EU Parliament elections scheduled for May 2014. A number of member states, including the UK, are concerned that some elements of a proposed EU data protection directive could have a negative effect on business. Smaller businesses could be faced with fresh administrative burdens undermining the benefits of the digital economy that is being built in the UK and other EU member countries. Although the legislation would affect the world's largest internet companies, such as Google, Facebook and Yahoo, it would also have ramifications for small businesses.

Family history research cannot be done without access to birth, marriage, divorce, death, census, voting and property records and a myriad of other records upon which genealogists depend.

On October 21, the EU's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) voted on an amended Proposed Data Protection Regulation. The approximately 4,000 proposed amendments were consolidated into 104 compromise amendments of which the overwhelming majority were adopted. At the time this article went to press, we have not been able to read the revised proposed data protection regulation, as it was not posted yet to the EU Committee website.

The press release from Viviane Reding, the EU's vice-

president of the Council, summarized the LIBE vote which passed overwhelmingly (49 votes in favor, 1 against and 3 abstentions). The principle of the "right to be forgotten" was amended to also include the "right to erasure." The next steps include LIBE members Jan Philip Albrecht of Germany, member of EU Parliament, and Dimitrios P. Droutsas of Greece, member of EU Parliament, to negotiate with members of the European Union Parliament. It will take time to "lobby" the heads of state of the 28 EU countries—and may be the reason Chancellor Merkel has agreed to delay the vote—as the earliest the full EU Parliament may meet to vote on the proposed regulation is Spring 2014. The press release is available at http://tinyurl.com/l3unnam.

The focus of the negotiations will be the EU's critical issue of "one-stop-shop." The one-stop-shop principle would change the current rule that requires multinationals processing personal data established in several EU member countries to comply with the local requirements of each jurisdiction. The proposal would instead have a supervisory authority that the "main" establishment be in control. This issue is controversial among the various EU nations. The next scheduled meeting of the Justice Ministers on the data protection regulation relative to the "one-stop-shop" is December 5–6, 2013.

In addition to one law for all 28 EU members, one of the pillars of the proposed regulation is that non-European companies will have to adhere to European data protection law if they operate in the European market. This proposed regulation applies to the processing of personal data of subjects residing in the EU by a controller not established in the EU, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behavior. There are onerous penalties included if a data processor violates the provisions of the regulation—including fining companies up to €100 million for breaching data protection rules. Data processors we are familiar with for genealogical research that are not based in the EU—such as Ancestry.com, MyHeritage, and potentially the SIGS that have data or indexes on websites—may be affected.

Under the "right to be forgotten" and the "right to erasure," if the individual no longer wants his or her personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from the system. In some cases, a legitimate reason exists to keep records in a database. Viviane Reding gave newspaper archives as a "good example" for retaining information. This principle permits citizens to obtain from third parties (to whom the data have been passed) the erasure of any links to, or copy of, or replication of that data. It is clear from Reding's statement that the right to be forgotten cannot amount to a right to rewrite or erase history. This is essentially what Lord McNally wrote to the IAJGS in response to its letter of concerns with the proposed regulation (see below). Vice-president Reding commented that genealogical research was not specifically examined, and no specific provision concerning genealogical research is in the proposal.

While IAJGS was advised by the UK's Ministry of Justice Lord McNally that the intent of the regulation is to protect the living, no explicit exception for genealogical records under Article 83 which covers historical records—therefore, the genealogical community must remain vigilant. The Ministries of Justice from Germany and Spain also replied to IAJGS's letter indicating that genealogical records should be treated as "status quo." One of the genealogical communities' concerns is the EU principle of the "right to be forgotten" and now also "the right to erasure." A living person may request to have their data removed or "erased"—and if they do what does that do for future genealogists who will research those who are currently living after they are deceased? If genealogically relevant data is permitted to be "erased," the future of genealogical research may well be hampered.

U.S. National Security Agency (NSA) spying is a pivotal issue with the EU on data protection and more and has affected the overall issue of data privacy.

The EU's proposed data protection regulation's primary focus is protection of the individual's privacy.[3] As currently proposed, the regulation is imprecise and has inherent flaws that will impede genealogists' access to family research. The section of the proposal of most concern to genealogists is Article 83, "Processing for historical, statistical and scientific research purposes." While IAJGS has been advised that the regulation's intent is to protect the living, the proposed regulation will apply to organizations based outside the EU if they process personal data of EU residents. The EU defines personal data as "any information relating to an individual, whether it relates to his or her private, professional or public life. It may be anything from a name, a photograph, an e-mail address, bank details and posts on social networking websites, and medical information or a computer's IP address."[4]

Genealogical Concerns. As currently proposed, the regulation goes too far from its original intent of protecting an individual's privacy by preventing public access to valuable information, and if adopted as proposed—based on the original draft as the compromise language has yet to be released to the public—may have a chilling effect on access to genealogical records, both historical and current. This could affect not only genealogical records organizations such as Ancestry.com, Family Search, Findmypast and MyHeritage (which have records available from many of the 28 EU member countries—including more recent records), but also the many special interest groups that have placed indexes or digitized records online—whether JewishGen.org or individual Special Interest Groups (SIGs)—such as Jewish Records Indexing-Poland, Gesher Galicia and the LitvakSIG.

While being told only records of living persons in the

(continued on page 49)