Closing Death Records: “Silver Bullet” or Dead End? _Moss_Outline

The proposed presentation will be an updated version of a preliminary report on an on-going case study reflected in the paper that follows which was presented at the ID360 Conference sponsored by the University of Texas Center for Identity in May 2015 and again scheduled to be presented at the University of Kansas School of Law on the 6th of July 2015.

ID360 2015: The Identity Economy

Closing Death Records:
"Silver Bullet" or Detour?

A case study of
Section 203 of the Bipartisan Budget Act of 2013

Submitted April 10, 2015
By
Frederick E. Moss, JD, LL.M.
access@fgs.org
972-679-5377

Executive Summary

For more than a year, the genealogical community has been working with the National Technical Information Service in crafting regulations implementing Section 203 of the Bipartisan Budget Act of 2013, as written, and suggesting areas where changes in legislative language might enhance the ability to (1) achieve the stated goal of reducing the opportunities for identity theft**,** and (2) minimize the unintended adverse consequences of limiting access and content available to legitimate users. Further question whether these provisions belong in permanent legislation and suggest ways of assessing their effectiveness and the impact of more targeted measures. A further rigorous case study may be appropriate.

Introduction

I serve as the legal advisor to the Federation of Genealogical Societies and as a member of the Records Preservation and Access Committee more fully described as follows: The Records Preservation and Access Committee, (RPAC) is a joint committee of the National Genealogical Society (NGS), the Federation of Genealogical Societies (FGS), and the International Association of Jewish Genealogical Societies (IAJGS) as sponsoring members. The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), International Commission for the Accreditation of Professional Genealogists (ICAPGen), and the American Society of Genealogists (ASG) also serve as participating members. RPAC meets monthly to inform and advise the genealogical community on ensuring proper access to vital records and on supporting strong records preservation policies and practices at the federal, state, and occasionally the local level.

Our activities are reflected in the RPAC Blog hosted on the FGS web site at:

http://www.fgs.org/rpac/ .

How the Internet is changing our lives

We live in a world of "Big Data" in which more and more information is being created, more is being digitized and much being made available on the internet. It is now possible to use that data in previously unimaginable ways to extract knowledge and information. We love it. We depend upon it. It is driving our economy. But we also worry about the privacy, civil liberties, and democratic implications of these developments.

Genealogy operates at the cutting edge of these concerns. It is a data dependent exercise and it is an increasingly internet dependent exercise.

Scourge of Identity Theft

We share the internet with others also cursed with thieves who would exploit the anonymity frequently available there for sometimes despicable purposes. The impact of measures occasionally taken in response to this threat may fall upon the thieves but are as likely to adversely burden the legitimate users of data valuable enough to have be collected and preserved for praiseworthy purposes.

Initiatives to restrict access to records – Targeting the Data

In recent years we have seen more than a thousand legislative initiatives impacting access to records at the Federal, state and local levels, the vast majority of which would have had the effect of limiting that access for genealogical and other purposes. The rationale used to justify these measures suggests an almost reflexive belief that the best or only way to prevent the fraudulent use of such data by identity thieves is to close the records. This logic carries with it the unstated assumption that no harm or loss accompanies such closures.

Section 203 of the Bipartisan Budget Act of 2013 represents the most dramatic modern example of this approach at the federal level. Although it presented as an access issue, the provisions that reduce the display of historically available data elements and diminishing the content of the Death Master File trigger equally significant preservation concerns.

Since 2011, representatives of the genealogical community have monitored approximately a dozen Congressional hearings in which the scourge of tax fraud by identity theft has been raised. In most of those hearings, although not asked to actually testify, we have provided Statements for the Record suggesting that better alternatives might be available. http://www.fgs.org/rpac/ In these hearings, we were frequently informed of the acknowledged harm resulting from the theft in the context of explaining why consideration was being given to dismantling, closing, or otherwise limiting access to the Death Master File. Rarely, if ever, during a hearing was concern expressed (or even awareness of the possibility) that costs might be paid or harm might be done by closing the record.

In the process of fulfilling their mandate to develop the Certification program required by this statute, NTIS has provided a forum for those adversely impacted by the limitations of access to the DMF to begin to document the fact that records closures come at a price. Their concerns are recorded at http://www.regulations.gov/#!docketDetail;D=DOC-2014-0001 and highlighted in

the RPAC Blog at http://www.fgs.org/rpac/2015/04/01/dmf-comment-period-onproposed-final-rule-closed-30-march/
.

Genealogists share Privacy Concerns

Family Historians and their families are as vulnerable to the predations of identity thieves as any other citizen. Our names appear on the lists of those compromised by reported major data breaches at Target, Home Depot, and Anthem among others. Some of our colleagues have been issued PINS by the IRS to be used in filing their 2015 returns because fraudulent tax returns using their information have been filed by identity thieves in the past. Those who believe that genealogists are reckless with Personally Identifiable Information might be pleasantly surprised at some of the measures taken by websites and individual researchers.

Be assured that the genealogical community is prepared to be supportive of measures which actually protect us from identity theft. We fervently wish that we could believe that the measures mandated by Section 203 of the Bipartisan Budget Act of 2013 limiting access and content of the Social Security Administration's Death Master File would have that effect. Our analysis has suggested otherwise.

Three Questions for Legislators

When issues first arise, decision-makers will rarely have access to the information needed to make an informed judgement or craft the appropriate legislative response. At this early stage, asking the right questions may be critical. We would urge consideration of at least the following:

A. Is the best [or only] way to stop ID thieves closing the records they might have used?

B. Can access to vital records or the Death Master File be closed (or limited) without harm or cost?

C. Is it impossible for you to believe that more effective alternatives to closure can be found?

Resolving "Big Data" issues

These questions are difficult to address in a vacuum, especially in the absence of data and input from a broad spectrum of stakeholders. As a society, we have barely begun to even ask the right questions, much less agree upon the answers. What information should be kept public? Which private? What are the rules to be? How are those rules to be developed? Our thesis is that an enduring resolution of these questions can best be achieved by a process that includes a searching dialogue among (1) the subjects of the data, (2) those who create, aggregate or

maintain the data, and (3) those who might use the data for a variety of legitimate purposes. The NTIS process has provided one such forum.

Would that more of this process been observed before legislative language had been enacted limiting access to the Social Security Administration's Death Master File, a little known but highly effective fraud prevention resource when used. Ironically most of the legislative proposals to limit the use of the DMF were prompted by incidents in which agencies such as the Internal Revenue Service or the U.S. Office of Personnel Management (OPM) should have used the DMF but had failed to do so.

In fact, if thieves had attempted to use social security numbers taken from the Death Master File in most commercial transactions, they would have been rejected. In their rush to expedite refund payments in 2011, the IRS was not using the DMF to flag suspicious cases or to help validate legitimate returns. OPM continued to mail federal employee retired pay check to the last known address even after they had died, because they were not checking the DMF. When used, the DMF (listing what should be inactive SSNs) is among our most effective fraud prevention tools.

We thank the National Technical Information Service (NTIS) of the Department of Commerce for the exemplary manner in which they have sought to craft regulations implementing their statutory mandate, for conducting the most rigorous review of the legitimate uses of the Death Master File (DMF) conducted thus far, and for providing stakeholders a forum in which to describe the impact of and offer suggestions to improve various approaches to be taken. They have provided a commendable demonstration of what a robust notice and comment process looks like, an example truly worthy of emulation.

What Have We Learned?

Timely information on death is of critical importance across a broad spectrum of endeavors that exceed those of genealogists, the financial interests represented at last year's public hearing, or even those of the 114 entities participating on-line.

When representatives from the financial sector voiced concerns about the 2011 removal of data provided by the States from the DMF, and feared a further degradation of that resource, they spoke for all traditional subscribers. Members of the research community had previously voiced similar concerns: http://www.nytimes.com/2012/10/09/us/social-security-death-record-limitshinder-researchers.html

We were all particularly alarmed by the possibility that administration decision-makers believed that alternatives to the DMF were available and that historical users of the DMF could readily find what they needed from other sources. Those in attendance at the 4 March 2014 public hearing suggested otherwise, a posture also adopted by the Council of Professional Associations on Federal Statistics in their recent comment at DOC-2014-0001-0061.
For most financial purposes, verifying that an individual already known to them has died enables the enterprise to begin "closing the file" on the deceased individual. For researchers (especially for genealogical projects) finding an individual referenced in the DMF is more likely to be the beginning of the project with a need for them to continue the search for other relatives through

the DMF. Locality information in the DMF suggests where one might look for additional documentation.

What Have We Lost?

Limitations on access and the reduced utility of the Limited Use DMF have already impeded the work of those genealogists:

- Assisting the Department of Defense in locating heirs for the repatriation of remains from previous wars,
- Assisting county coroners in the identification of unclaimed persons,
- Working with attorneys in locating missing and unknown heirs involving estates, trusts, real estate quiet title actions, oil and gas and mineral rights, and other similar legal transactions,
- Tracing and tracking heritable medical conditions where finding distant cousins can facilitate early treatment and possibly prevent a premature death
- Repatriating stolen art and artifacts, and
- Identifying American Indians, Native Alaskans, and Native Hawaiians to determine eligibility for tribal benefits and blood quantum when required.

The academic research community and those engaged in federal program evaluation have provided even more dramatic examples.

The Path Forward – A Proposed Case Study

The way in which the challenge of tax fraud by identity theft has evolved in recent years presents a unique opportunity to evaluate the effectiveness of several approaches to combating it.

1. Initial baseline period – TY 2010, TY 2011

During the period immediately preceding December 2011, the DMF was widely available on the internet and the IRS was doing minimal filtering that might have flagged fraudulent refund claims. Apparently the IRS was not filtering against the SSA's Death Master File in 2010 and 2011 before issuing potentially fraudulent refund checks. The data necessary to initially determine the nature and magnitude of tax fraud by identity theft cases first coming to public attention in 2011 would not become available until the fall of 2013 with the publication of the report of the Treasury Inspector General for Tax Administration drawn from the TY 2011 data, issued September 20, 2013 and found at: http://www.treasury.gov/tigta/auditreports/2013reports/201340122fr.pdf . The attached chart (Figure 4) is taken from that report and provides a potential baseline for assessing the effectiveness of subsequent steps taken to improve filters used to flag suspicious returns before processing them for payment.

The chart below is drawn from Tax Year 2011 tax returns, those filed in early 2012. Please note that the only SSNs that would appear in the DMF/SSDI would be the "Deceased" Category. The IRS was utilizing a limited screening filter that appears not to have used the DMF to flag for special attention returns citing the SSNs of deceased individuals.

Even with deceased SSNs fully "exposed" during 2011, the 19,102 suspicious returns listed above represented less than 2% of the 1,086,998 potentially fraudulent returns filed in 2011. Limitations on access to the DMF will have no impact on cases representing the misuse of the SSNs of living individuals (all the other categories in the chart above and representing the other 98% of the cases) nor SSNs of deceased individuals from compromised medical records.

2. Period 2 – December 2011 to April 2014

In December 2011, genealogical web sites began masking the SSNs of recently deceased persons and the IRS reportedly significantly improved their software filters. The IRS effort has included continuing refinement of the filters to flag returns demonstrating characteristics of those found to have been fraudulent. Thieves change; we learn.

3. Period 3 – April 2014 to present

In April of 2014, the limitations on access and content of the DMF mandated by the Bipartisan Budget Act of 2013 are implemented.

Having a comparable chart for TY 2012, TY 2013, TY2014, (and possibly a look back to 2010) could give visibility over where our challenges still lie, what measures are working, and which measures may be of only marginal utility. I appreciate that it may take a year or more for a suspicious return to be fully resolved so we may be asking for TIGTA to undertake an ongoing project.

A rigorous analysis could suggest that the measures taken by the IRS, together with those measures taken by genealogical entities, may have largely intercepted this particular form of identity theft in advance of this legislation. It might also suggest better approaches to intercepting the far more prevalent misuse of the SSNs of the living.

Conclusions

1. NTIS has implemented the statutory mandate, as written.

Operating within the constraints of their current statutory mandate, there is little more that NTIS can do to create a more functional Certification program. We are prepared to work with appropriate Congressional committees to suggest more effective statutory changes.

Deferring to the possibility that members of the financial community engaged in fraud prevention may assert otherwise, major enterprises likely will be provided the access they need to the available DMF content.

But, that content is no longer as comprehensive as it once was prior to the 2011 decision to withhold state-provided content. Financial services representatives voiced particular concern that the on-going withholding of state data will further degrade the value of the DMF resource and make their fraud prevention efforts less effective.

2. This statute may not be the final answer.

Limiting access to the DMF is not the "silver bullet" solution to the scourge of tax fraud by identity theft. It could do more harm than good.

Our strongest message is that steps already taken by the IRS and genealogical entities to protect SSNs listed in the SSDI may have largely intercepted this particular form of identity theft in advance of this legislation. Its primary impact may be to burden legitimate users both operationally and financially. Our suggestion for a case study provides a way to assess the effectiveness of various measures taken.

3. The statutorily mandated Limited Use Death Master File is inadequate.

Those of our genealogical colleagues who have been certified and begun to work with the LUDMF resulting from this effort report that the search engine and the data elements displayed

for this product no longer meet our needs. Genealogists were not the only DMF users concerned that the DMF is being incrementally degraded. The new limited access DMF needs a much improved search engine.

4. The path forward:

The Genealogical community is anxious to work with all interested parties in an effort to develop a truly comprehensive nation-wide death index. The concerns of State Vital Records officials that led to the ongoing removal of state data from the DMF in 2011 must be addressed.

We recognize a need to work with the Congress and other interested parties to improve existing measures and suggest additional approaches to combat the scourge of identity theft.

The SSNs of living people will remain vulnerable as long as the IRS mandate is to rush payments of tax refunds before information returns can be compared with the submitted return to assure its validity.