# The Duty to Remember v the Right to be Forgotten: Holocaust Archiving and Research, and European Data Protection Law

**ARYE SCHREIBER**

**Abstract**

European data privacy laws arose largely in reaction to the horrors of authoritarian rule generally, and the Holocaust specifically. Privacy and data protection have consistently been a barrier to Holocaust justice. The Data Theory of the Dutch Holocaust, widely cited as a justification for EU data protection law, has long served as a smokescreen for extensive collaboration with the Nazis. The largest Holocaust archive was inaccessible to victims and researchers for decades, principally on account of privacy considerations. Privacy prevented publication of indictments of Auschwitz SS, and served as principle grounds for non-cooperation of banks and insurance companies in restitution of property of Holocaust victims and survivors. The EU's new data protection regulation (GDPR) and its new Right to be Forgotten threaten to pose further challenges to Holocaust research, and bold legal positions may need to be taken in order to avoid Holocaust research being stifled, as several approaches are analysed. Holocaust justice has been central in informing legal responses to other atrocities. For all its importance, data protection law must not be allowed to prevent justice in human-rights abuses, nor to prevent proper research and victims' healing.

**Keywords**

Privacy, data protection, archives, GDPR

## Introduction: Holocaust Jurisprudence and Privacy

There is a rich and growing literature of jurisprudential responses to the Holocaust,[1] and there is a huge corpus of scholarship on privacy law.[2] This article

[1] Byrne, "Legal Theory and The Holocaust", p. 373.

[2] The present article considers privacy in the most common meaning: protection of personal information. Privacy and Data Protection are very closely related, and for the present purposes synonymous, concepts. For some taxonomies of privacy, see Solove, *Understanding Privacy* and Mills,

seeks to demonstrate that privacy has played a major role in post-Holocaust justice, and more particularly in its obstruction. Several have noted the connection between privacy and the Holocaust, or more generally between privacy and twentieth century totalitarianism in Europe, and the development of European privacy law is often regarded as a reaction to abuses of data in the Holocaust.[3] This has sometimes been seen as a "hidden agenda of discouraging a recurrence of the Nazi and Gestapo efforts to control the population",[4] and sometimes considered not a hidden agenda but rather "one of the prime motives for the creation of data protection laws in Continental Europe."[5] But as is shown below, privacy has repeatedly been used as a means to obstruct post-Holocaust justice. Many parties – banks, insurance companies, courts, law enforcement, publishers, the International Red Cross, and others – have claimed that privacy rights prevent their disclosure of information that serves Holocaust justice and restitution. In some cases, privacy was or could have been a legitimate concern. However, there emerges a pattern in which these parties use privacy as a tool to obstruct various processes of Holocaust justice, and their bad-faith abuse of privacy is demonstrable, as famously represented by the saga of Christoph Meili, the security guard at UBS who whistle-blew on the bank's intended shredding of Holocaust-era account papers.[6] Privacy rights and European data protection laws have repeatedly and extensively been used to prevent and delay Holocaust justice and restitution.

The importance of a more refined and just consideration of privacy rights in relation to the Holocaust is high not only for the Holocaust justice. The Holocaust is perhaps the most studied of atrocities, especially with reference to law, and Holocaust jurisprudence is educating and influencing the search for truth, justice and healing following many other atrocities and human rights violations, from Armenia and Ukraine to Rwanda and the former Yugoslavia. Holocaust awareness has become an issue of international significance in the fight against racism in thought and action, as illustrated, for example, by the United Nations General

*Privacy: The Lost Right*. Other interesting aspects of privacy, such as self-determination, certainly warrant consideration in a Holocaust research context, and I leave that for another opportunity.

[3] Some sources are discussed in detail – including the opinion of an EU national data protection authority. A small selection of sources for the Nazi abuses of data in the Holocaust as the grounding for EU data protection law demonstrates its prevalence: Bloch-Wehba, "Confronting Totalitarianism at Home", offers some nuance on the connection between Nazi philosophy and activity and EU data protection law, but generally supports the direct influence, citing several additional authorities (fn.82); also Bignami, "European Versus American Liberty", p. 688. Cf. Wittmann, "The Two Western Cultures of Privacy", especially at pp. 1189-1190. This view has also become common in law textbooks, e.g. Lloyd, *Information Technology Law,* p. 23. See also González Fuster, *The Emergence of Personal Data Protection*.

[4] Flaherty, *Protecting Privacy,* p. 373.

[5] Bennett, *Regulating Privacy*, p. 30, citing Flaherty's summary of a 1984 data protection conference.

[6] See details in Bazyler, *Holocaust Justice: The Battle for Restitution in America's Courts*, p. 19.

Assembly Resolution on Holocaust denial,[7] and the European Council protocol on xenophobia online.[8] Holocaust jurisprudence trickles down into a broad array of legal processes and institutions, and therefore the more developed and refined it is, the greater its impact. It is hoped that the present enquiry will contribute to the pool of tools and knowledge that enable truth to be revealed and justice to be done and healing for the victims following any and all atrocities, and in particular for a more nuanced and just treatment application of privacy rights to prevent those rights from being abused so as to protect perpetrators and beneficiaries of atrocities.

One of the great challenges of Holocaust-related legal issues is that the Holocaust was unprecedented in the scale and scope of perpetrators and victims, in the convergence of ideological and economic motives, and in the involvement and support of state institutions, general population and – especially relevant in the present context – the legal community. Legal reactions to the Holocaust were also largely without precedent in their intensity and scope: the Convention on Genocide[9] and the Universal Declaration of Human Rights were written in reaction to it;[10] the International Military Tribunal (IMT) at Nuremberg was likewise unique, and an important precedent that largely led to the founding of the ICJ;[11] and the Holocaust has led to sui generis legislation such as Holocaust Denial laws. But privacy, by contrast, is a very ordinary legal concept: it has various civil, criminal, commercial, social and human rights aspects to it, and it was well documented and applied long before the Holocaust, in the US and in Europe – including in Germany. The Holocaust had several very important connections with privacy, not all of which can be discussed here. One important topic, beyond the rubric of this article, is the meaning and significance of privacy in Nazi ideology, an ideology in many ways opposed to notions of a right to be let alone, or as Mills put it: "where the state has a powerful enough grip on its people, ideology can overtake and eliminate any semblance of individual privacy."[12] This article will focus on particular aspects of privacy in connection with the Holocaust, namely: the ways in which privacy rights have obstructed Holocaust accountability, justice and restitution. In the next section, I will discuss the way in which the lack of data protection has been used to smokescreen massive complicity in Holocaust atrocities, in particular with reference to the "data theory" of the Dutch Holocaust, which had a direct and

---

[7] Resolution adopted by the UN General Assembly on Holocaust denial (A/RES/61/255, 26 January 2007), http://www.un.org/en/holocaustremembrance/docs/res61.shtml.

[8] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.1.2003. The Explanatory Report explains that Holocaust Denial is the archetype instance of genocide denial: paragraphs pp. 39-42.

[9] Cooper, *Raphael Lemkin.*

[10] Vrdoljak, "Human Rights and Genocide", pp. 1163-1194.

[11] Findlay, *International and Comparative Criminal Justice*, p. 19.

[12] Mills, *Privacy: The Lost Right*, p. 22, footnotes omitted.

marked influence on the OECD privacy principles and EU Directive 95/46. In another section, the International Tracing Service of the International Committee of the Red Cross (ICRC), an organization charged with care and use of the massive archives of documents seized from Nazi Germany, likewise blocked initiatives in restitution, history and justice with claims of privacy. Next, there is a brief discussion of ways in which privacy prevented justice from being done and being seen to be done in both research and judicial processes. Likewise I will examine how privacy was repeatedly abused by banks and insurers hiding enormous assets from survivors and victims and their heirs.

Before delving into these details, there is one important point that needs consideration. Privacy is today rightly protected in international legal instruments and national laws. This article does not argue that the right be unceremoniously waived aside in instances of Holocaust justice. The argument is much more nuanced than that. Privacy became a fundamental right in the EU only after the Holocaust, and largely in reaction to the Holocaust.[13] It is a human right and protects the dignity of the data subject. Ironically, in many cases it was allowed to prevent justice, and unquestionably harm the dignity of the data subjects, for example when Holocaust-era bank account and insurance policy beneficiaries' names were not published; though publication would be a *prima facie* violation of their rights, the banks and insurance companies made these claims to the beneficiaries themselves, where the beneficiaries could not provide documentary evidence of the account being in their name. In other words, the purpose of the law, the values underpinning it, and the events which inspired its formation, were all set aside as some very powerful organizations, like UBS and Credit Suisse, Allianz and Generali, claimed with brazen irony that they would protect their clients' privacy. Privacy laws protecting the account holders were used against the property rights of those same account holders. This, as one US congressional representative said, was "both Kafkaesque and a Catch-22."[14]

Privacy laws accept that data protection rights must not obstruct justice. For example, England's Data Protection Act 1998 stipulates (section 35) that "Personal data are exempt from the non-disclosure provisions where the disclosure is necessary… for the purposes of establishing, exercising or defending legal rights." Sadly, as will be evident in the following pages, in the actual instances in which privacy was an obstacle to Holocaust restitution, it was not out of concern for protection of privacy, but on the contrary as a means to protect assets or reputation obtained in violation of the property rights and the human rights of the same data subjects.

---

[13] See above note 3.

[14] Bazyler, *Holocaust Justice*, p. 195.

Thus the present author hopes that the role of privacy in post-Holocaust restitution and justice catalyses more nuanced and thoughtful consideration of privacy and the ways in which it can be prevented from blocking justice in other atrocities.

## The Data Theory of the Dutch Holocaust and European Data Protection Law

In this section, the Data Theory of the Holocaust of Dutch Jewry is considered. As detailed here, this theory – though it has gained widespread credence and is viewed by many privacy regulators and researchers as instrumental in the development of European data protection law – gives a skewed impression, ultimately serving as a smokescreen for some considerable moral and legal culpability.

Every few years, the Irish Data Protection Commissioner conducts a survey on data protection awareness among citizens. In response to one year's findings, the Commissioner created educational materials, to be used in schools, explaining the importance and role of data protection law. The publication – a novel and welcome idea – details some ways in which Nazi Germany abused data in order to perpetrate the Holocaust. The guide summarizes:

> "How did the holocaust occur on such a massive scale? How did the Nazi authorities know exactly who was Jewish? How were the Jews captured? How did the Third Reich identify popular Jewish residential areas? [The] Answer [is] DATA."[15]

The Commissioner explains that the Irish, and earlier European, legislation on Data Protection are reactions primarily to the Holocaust – a view rightly and widely supported by legal historians, who demonstrate that European privacy law, as well as the broader context of European human rights law, has been "shaped by this Nazi past."[16] In addition to discussing abuses in Germany, the Commissioner highlights wartime Netherlands as an example of data being abused in the Holocaust. Indeed, there is a commonly held view that the Dutch records fell into Nazi hands, such that the well-meaning Dutch inadvertently provided the Nazi monster with reams of data on the identity and whereabouts of their Jewish countrymen. The influence of this theory is not to be underestimated. By way of illustration, in a conference marking thirty years since the OECD Privacy Guidelines – arguably the

[15] https://www.dataprotection.ie/documents/teens/cspe%20resource%20booklet/Section_2_-_Privacy_as_a_Human_Right.pdf. In the original this text is presented in a flow-chart graphic; capitals in the original.

[16] Bignami, "European Versus American Liberty", p. 687, see generally note 3 above.

most influential of all privacy formulations – the chairman of the original expert committee, Michael Kirby, later a judge at the Australian High Court, related that during a conference open to the public, in which the then French President was present, a member of the public said as follows:

> "'Why, Mr. President, did so many refugees and Jews in France survive during the War? Why did so few resistance fighters and Jews survive in The Netherlands?', he said. 'It happened because, in the 1930s, The Netherlands government, with typical efficiency, had devised an identity card with a metal bar installed through the photograph. This was then the latest in secure technology. In France, we had an ordinary photograph, pasted on cardboard. It was easily imitated. Upon that difference hung the lives of thousands of good people. In France, they survived. In The Netherlands they perished. Efficiency is not everything. A free society defends other values. Personal control over data is one such value."

In his speech, Kirby added: "I never forgot the point which this contributor made in the presence of the French President."[17] Indeed, the identity card was very hard to forge. Jacob Lentz had been head of the Dutch population registries in the 1930s, and his proposals for identity cards were rejected as un-Dutch. The German occupiers, however, embraced his proposals enthusiastically, and in 1941 identity cards were issued with two photographs, fingerprints, signatures and more, all on watermarked paper.[18] Others emphasized not the data security of the Dutch identity cards but the sensitive information they included. For example, one scholarly paper that has been quoted repeatedly in this respect notes as follows:

> "Take as an extreme example the effort in the 1930s by the Netherlands to redesign their population information systems. The clear purpose of this endeavour was to improve administrative efficiency. However, part of the data that they collected, for innocent reasons, was each citizen's religious affiliation. Catastrophically, these data systems fell into the hands of the Nazis, and, arguably, as a result, Dutch Jews were killed at a much higher rate than any other Jews in Western Europe during the Holocaust.[19] This very small amount of data collected on Dutch citizens (representable by

[17] M.D. Kirby, "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy", Round Table on the 30th Anniversary of the OECD Guidelines on Privacy, 10 March 2010: http://www.oecd.org/sti/ieconomy/44945835.doc

[18] Wolf, *Beyond Anne Frank*, p. 71, citing Moore, *Victims and Survivors*.

[19] Citing: W. Seltzer and M. Anderson, "The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses", *Social Research*, 68, 2001, pp. 481-513.

a single bit), benign in one context, was re-purposed in deadly fashion in another context."[20]

This is the "data theory", and it has long been believed that Dutch population data was of particular help to the Nazis in their elimination of Dutch Jewry.[21] The meticulous records, complete with racial information, kept by the Dutch government seem to have contributed to the particularly high proportion of murder of Dutch Jews, as compared with other West European states. Truly, as German media theorist Wolfgang Ernst has asserted, "Archival memory became… an instrument in the National Socialist programme for annihilation of European Jewry"[22] – meaning that the archives and records became deadly, as they were used by Nazis to murder as quickly and efficiently as possible, as was the "IBM-Hollerith punch card system [which] made identification not only possible, but also lightning fast and efficient."[23] The secure cards, the racial data collected, the archives maintained, and the emerging data processing technology – all contributed to the massive murder of Dutch Jews. To be clear, alternate theories have been proposed, and each has some support; these include: the lack of organized resistance; the collaboration of the Dutch – who were "Germanic", in contrast with, say, the French; the geographical landscape that could not support hiding places; and more.[24] Though other factors contributed to the low survival rate of Dutch Jews, detailed Dutch records in Nazi hands made the task of annihilating Dutch Jewry much simpler than it would otherwise have been. This is rightly cited as an example of the dangers of sensitive information in autocratic hands.[25]

However, a very important clarification is in order; true as it may be that the Nazis could not have annihilated Dutch Jewry quite so effectively without access to those databases, making Dutch archives and records undoubtedly a part of the story, they remain but just one part. In the post-Holocaust years, the Dutch narrative told of a country taken over by the Nazi machine. The truth is much less flattering. Lazer and Mayer-Schonberger wrote that "Catastrophically, these data systems fell into the hands of the Nazis", but the Dutch data did not "fall" into German hands, nor was it taken. It was given. Dutch Jews, almost 10% of the pre-war Dutch population, were rounded up by Dutch policemen, put on Dutch trains driven by Dutch drivers, taken to concentration camps in the Netherlands–notably Herzogenbusch, Westerbork and Amersfoort, their property was looted by the

[20] D. Lazer and V. Mayer-Schonberger, "Statutory Frameworks", p. 368. See for example de Azevedo Cunha, *Market Integration*, p. 2.

[21] Seltzer and Anderson, *Using Population Data Systems*, at p. 311.

[22] Ernst, "Archival Action", p. 25; see Ketelaar, "Archival Temples", p. 226.

[23] Gilreath, "The Internet and Inequality", p. 535, footnotes omitted. See at length Black, *IBM and the Holocaust*.

[24] See Croes, "The Holocaust in the Netherlands".

[25] Spiekermann, *Ethical IT Innovation*, p. 49.

Dutch, and Dutch banks transferred their bank account balances to the Germans.[26] It may be speculated that the prominence of Anne Frank's story and diary has contributed to the notion that the Jews were well treated by the Dutch; after all, Anne was preserved by Miep Gies and others, and her diary ends before her apparent betrayal and transfer to Westerbork, Auschwitz and Bergen-Belsen. But she and her family were the exception for surviving so long in hiding, and ultimately they too were almost certainly betrayed by the Dutch, as were approximately one third of all Dutch Jews in hiding.[27] As famed Dutch historian and Holocaust survivor Presser wrote two generations ago:

> "Did not Dutch municipal officers collaborate in the registration of Jews and in placing the letter 'J' on Jewish identity cards? Did not virtually all officials sign the 'Aryan' declaration? Did not the Dutch authorities collaborate in the dismissal of Jewish civil servants? Did not the Dutch Bench implement many of the German decrees? Did not the Department of Social Affairs, the municipalities and the District Labour Offices allow themselves to be used to draft Jews to the work-camps? Did not the Amsterdam municipality play an important part in herding the Jews together? Did not the municipal transport system, the railways and the police, help in the deportations, and the gendarmerie help in guarding Westerbork camp?"[28]

Presser continued, and also provided damning evidence against members of the Jewish community. At any rate, it was the Dutch who oiled the wheels of the German Holocaust machine, and their detailed data which was enthusiastically handed to the Nazis was a part of that oiling.

Dutch recognition of collaboration at the level of national institutions was slow in emerging and inconsistent.[29] There is a well-documented longstanding failure by the Dutch government to face its complicity in the Holocaust,[30] and the data theory of the Dutch Holocaust has contributed to this failure by presenting an apparently plausible and now widely credited claim that Dutch data "catastrophically fell into Nazi hands", whereas the sombre truth, again, is that it was willingly handed over, like other assets, as clearly stated by various Dutch commissions of inquiry.[31]

---

[26] See at length Aalders, *Nazi Looting*.

[27] Wolf, *Beyond Anne Frank*, p. 81.

[28] Presser, *Ashes in the Wind*, pp. 273-4.

[29] As recently as 2012, the Dutch Prime Minister refused to acknowledge Dutch mishandling of the Holocaust; http://www.jpost.com/Jewish-World/Jewish-News/No-Dutch-apology-for-indifference-to-survivors, though earlier officials, including Prime Minister Kok, had expressed regret. See Gerstenfeld, *Judging the Netherlands*.

[30] Gerstenfeld, "Jewish War Claims".

[31] It is beyond the rubric of this article, but appears plausible, and worthy of further examination, that the Data Theory is essentially an exercise in "discontinuity', in the sense proposed by Fraser, *Law*

Dutch resistance, and especially Jewish resistance, made several attempts to destroy the data which was so convenient for the Germans. Karl Groger was a Viennese-born socialist, who was drafted to the Wehrmacht on Germany's invasion of the Netherlands, and was released on account of his being one-quarter Jewish. On March 27, 1943 several resistance fighters surreptitiously entered the municipal citizen registry in Amsterdam and ignited the filing cabinets in an attempt to destroy the data which facilitated the transports of Dutch Jews to Sobibor and Auschwitz. The raid was not ultimately effective, among other reasons on account of the existence of a duplicate registry,[32] and Groger and the others were all betrayed by fellow Dutchmen, and were executed. The registries continued to function – manned and operated by Dutch locals. In another raid shortly following the registry raid, Gerhard Badrian, a Jewish resistance fighter, led a raid on a state printing facility in The Hague, in which he was able to obtain thousands of blank ID cards which could then be used to forge ID.[33] Thus even at the time it was believed that the data in question was crucial to the German Holocaust efforts in Holland.

Whereas the Dutch resistance was ultimately unsuccessful in striking at the data Achilles-heel of the Germans, we may look to the Norwegian experience to see how the German reliance on data was also a weakness that could have, and ought to have, been exploited to undermine the Holocaust. Germany invaded and occupied Norway on April 9, 1940. Four years later, the German army sought to conscript Norwegian men to fight on the Eastern Front, and would use Norwegian government files including names, addresses, gender, and date of birth of citizens. The Norwegian resistance got wind of the plan and tried to destroy the files. That attempt failed, so the resistance instead destroyed the only two machines in Norway that could sort the data. "Without the ability to tabulate the population data, a Norwegian draft was too difficult to put into effect and the Nazi plan had to be dropped."[34] This was the Norwegians' answer to the German use and abuse of data against Norwegians, and the Dutch could have taken similar steps, but did not, and the data theory is thus a double-edged sword in the post-facto analysis of the use of Dutch data in the Holocaust. The Dutch government partially created the myth of data being grabbed by the Germans, its credibility buoyed by the quick destruction of incriminating evidence after the Holocaust. Though it was the Dutch government that destroyed the evidence:

*After Auschwitz*, meaning that this was yet another way for the Dutch, and Europeans generally, to dissociate themselves from the Holocaust horrors and their culpability: blame the data, not the Dutch.

[32] http://db.yadvashem.org/righteous/family.html?language=en&itemId=4042651

[33] Y. Lindeman and H. de Vries, *Resistance and Rescue*, p. 205.

[34] Bignami, "European Versus American Liberty", pp. 609-610, footnotes omitted, citing J. Bing.

> "After the liberation, the new Dutch government would seem to have decided that it did not want any incriminating material in the archives. Therefore the original archival material pertaining to the registration of the Jews, including the registration forms the municipalities had sent to the RvB, was destroyed. The central authorities then instructed the municipalities at the end of April 1946 to send for destruction the population registration cards that were marked with a 'J' for 'Jew'."[35]

Data protection, the main element of European privacy law, owes a lot to these Holocaust experiences, but data protection laws formulated ostensibly in reaction to Holocaust-era German abuses are perpetuating a gross misrepresentation that data "fell" into the wrong hands. Data, its protection and its abuse, has certainly played a significant role in genocide and mass human rights abuses throughout the twentieth century, including in Rwanda, Iraq and Bosnia,[36] making it imperative that the right lessons from the Holocaust experiences be learned and applied. One lesson is that sensitive data ought not to be freely collected and must be carefully protected, and this is the lesson reflected in European data protection law. Another lesson, one that has not been learnt and which many have a strong interest in avoiding, but which is central to this article, is that a "data theory" must not be allowed to smokescreen complicity and culpability, which can lead to a comprehensive and persistent failure of justice. Rather, where data has been abused, this ought to lead to a thorough investigation of the circumstances of such abuse, and lead to justice; as in the Dutch and other Holocaust experiences, it may well transpire that without extensive collaboration with the abusers, the data itself may have had little significance.

## Post-Holocaust Privacy: Obstructions of Justice at the International Tracing Service

The 27 kilometres of archive shelves at Arolsen, Germany, under the aegis of the International Tracing Service (ITS), on behalf of the International Committee of the Red Cross, form the most complex Holocaust archive.[37] The 1955 Bonn Agreement, governing its member states' commitments to ITS, stipulates in its preamble that the agreement is made "…for the purpose of tracing missing persons and collecting, classifying, preserving and rendering accessible to Governments and interested individuals the documents relating to Germans and non-Germans

[35] Croes, "The Holocaust in the Netherlands", p. 495, citing Circular (26-4-1946) of the RvB – Rijksinspectie van de Bevolkingsregisters, or "Inspector of Registrees".
[36] See Seltzer and Anderson, *Using Population Data Systems* and Allen, *Unpopular Privacy*, p. 145.
[37] McDonald, "Reconciling Holocaust Scholarship".

who were interned in National-Socialist concentration or labor camps or to non-Germans who were displaced as a result of the Second World War."[38]

In the 1950s, the Arolsen archives were shared with the US National Archives and with Yad Vashem,[39] but from the 1960s onward ITS would only provide information to victims and their families. By fin de siècle there were growing calls for the archives to be opened and shared without limitation – as Eastern Block survivors sought information, and as survivors generally knew their time was short. Congress, the US State Department, the European Parliament and others appealed to ITS. The German government was persistently resistant to opening up the Arolsen archives, largely based on the potential for violations of privacy. One newspaper reported:

> "The German government says it is committed to opening the archives, but not before privacy controls have been put in place. This is complicated because the privacy laws of many countries must be reconciled, a German foreign ministry spokesperson said. 'Before opening the archives to researchers indiscriminately, questions of privacy and liability for the misuse of this sensitive data needs to be addressed.'"[40]

It is not entirely clear whose privacy was ostensibly being considered. Clearly opening the archives could lead to further embarrassment for many Germans for their, or their relatives', Nazi activity. With its defeat, Germany's state archives were promptly accessed by the Allies, and made available to the IMT, and to other intelligence, legal and historical researchers. State archives that would ordinarily have been sealed for decades were opened in near real-time, such that at "least two successive generations of Germans were then permanently confronted with this open archival evidence of war crimes, the Nazi involvement of parents, and so on."[41] German law and policy, and Cold War exigencies, greatly muted the effects of this evidence, allowing all but a handful of Germans to get on with their lives. This must be understood in the context of Germany's sophisticated and novel way of dealing with the guilt of the Holocaust, as well as America and West Europe's need to win Germany and the Germans over in the Cold War. At the state level, Germany has been unprecedented in openly accepting culpability. Derrida has detailed the ways in which states erase and obscure their foundational, violent, lawless periods. West Germany did the opposite, and legally mandated remembering its violent past:[42] in

---

[38] https://www.its-arolsen.org/fileadmin/user_upload/Dateien/gesetzestexte/BA_1955.pdf.
[39] For more historical details of ITS, see Waltzer, "Opening the Red Cross".
[40] http://www.theguardian.com/world/2006/feb/21/highereducation.secondworldwar.
[41] Ernst, *Digital Memory and the Archive,* p. 202.
[42] Douglas, "Wartime Lies", p. 373, footnote omitted. Derrida himself was evicted from school in Algeria when antisemitic Vichy rules were implemented there in 1942.

1985 West Germany criminalized Holocaust-denial.[43] But Germany also imposed ever stricter privacy constraints, and these may be viewed as going hand in hand. The state accepted responsibility for the Holocaust, and determined that the Holocaust is a fact of law; but the embarrassment of the Holocaust, trials of thousands of Nazis, endless revelations of atrocities, and other painful steps could and would be avoided as far as possible. This is not to claim that privacy laws were passed with that conscious motive, though it is conceivable that it was a factor; rather, the state took responsibility at the national level, while sheltering its citizens from facing the ghosts of their personal pasts, save in a very limited number of extreme cases, and even then – as for example in the Auschwitz Trials discussed below – there were very limited ramifications. The German data protection regime provided a counter-weight to the Holocaust denial laws, perhaps shifting the focus of post-Holocaust justice from perpetrators of the past, to deniers of the past. Germany gained penance as a state, but would not repeatedly be embarrassed by the trials of many thousands of individual Germans. This balancing act seems to have largely animated public reactions to the Auschwitz Trials and in general the West German reaction to Nazis: "By identifying and prosecuting the 'worst' Nazi perpetrators, the Federal Republic indicated the boundaries of what was considered politically and morally acceptable without overly jeopardizing the political loyalty of millions of former Nazis by placing them at risk of either judicial prosecution or symbolic condemnation."[44] By the 1990s, the political power of former Nazis was not decisive, but ITS threatened to reveal a lot of pertinent information concerning a very large number of Germans at a time when the German people had rehabilitated its reputation and been reinstated in the community of nations. ITS was established and governed by international treaties, but located in Germany, subject to German law, and largely controlled by the German government. Understandably, the latter would work to avoid the traumatic effects of the opening of the archives on yet another generation, and privacy was a very convenient excuse for preventing the archives from reaching the public. This delicate status quo was threatened by the ITS archive.

The ITS privacy controversy slowly erupted:

> "Director Biedermann and several IC member countries 'reportedly blocked passage of the proposal' citing privacy issues and the original Bonn Agreement mandate (Belkin, 2007, p. 8). The argument shifted to privacy when those opposed to the proposals argued that sensitive personal information would be released and would violate individual rights while those in support of the proposal argued that 'the records provide unprecedented and invaluable first-hand documentation of the crimes perpetrated by the Nazi regime and

[43] *Strafgesetzbuch* (Criminal Code), s. 130.
[44] Pendas, "I didn't know", p. 432.

should be opened as soon as possible to allow for research collaboration with the remaining survivors…' (Belkin, 2007, p. CSR-3-4)."[45]

The "highly controversial Charles-Claude Biedermann began his reign of over 20 years in 1985. Under Biedermann, access to ITS files became increasingly restricted. Visitors were now only allowed to see the famed Index, and some of the buildings were off limits without the director's express authorization."[46] In the following years, the Soviet archives and borders opened up, and Eastern European victims began using ITS services, but Biedermann resisted mounting pressure to open the archives to research.[47]

The archives were opened only after Paul Shapiro, director of the Center of Advanced Holocaust Studies at Washington DC's United States Holocaust Memorial Museum ('USHMM'), took leadership of the cause, got support from the US House of Representatives, and "went so far as to argue that sealing off the archives was a form of denying the Holocaust, that in persisting in this closed-door policy the Germans could not avoid a second Holocaust" and similar claims. The German government withdrew its objections in early 2006; Biedermann was fired and the archives opened in June 2008.[48] Even then, Shapiro and USHMM were not able to put all the material online, for two reasons; one was the technological challenges involved; the other was that privacy "concerns continue to shape how the materials must be handled. Confidential materials about specific individuals (like objects of medical experimentation) clearly require protection, and the [International Committee of the Red Cross, which manages ITS] ruled that member governments must "take into consideration the sensitivity of certain information" under national privacy laws."[49] Ultimately the solution to the privacy conundrum was to allow the material to be published in the Commission's member states, subject to the privacy law in each respective member state.[50]

But years before the controversy became acute, privacy and confidentiality were apparently overprotected. In a piece published in 1993, Biedermann wrote: "Since it came into being, the ITS has issued over 7.2 million pieces of information and opened two million files to do so. In all its work, care is taken to protect people's right to privacy. Confidential data remain confidential: information is given only to the individuals concerned or their assigns. When tracing is successful and a person is found, the address is passed on to the enquirer only with that

[45] Brunelle, "A Brief Historical Evolution".
[46] Dreyfus, "Opening the Nazi archives".
[47] Leading to interesting rumors verging on conspiracy theory, *ibid*., p. 7.
[48] http://www.spiegel.de/international/fifty-million-nazi-documents-germany-agrees-to-open-holocaust-archive-a-411983.html
[49] Waltzer, "Opening the Red Cross", p. 167.
[50] Belkin, "CRS Report". See also Amending Protocol 26 November 2007.

person's express consent."[51] Thus Biedermann, even in the early years of his ITS leadership, emphasized the role of privacy, and the extreme caution ITS would exercise in connecting relatives, for example.

Let us take a thorough and un-cynical look at Biedermann's position. Arguments have been made for ITS' immunity from German privacy law based on its status as an international organization,[52] and adopting such a position would obviously have greatly alleviated the privacy challenge involved in opening the archives, and Biedermann could have advocated for such a position. But assuming that ITS was not immune from German privacy law, Biedermann's assertion that privacy was a real impediment to simply opening the archives without limitation was basically correct, at least as an opening position. Arolsen is in the German state of Hesse, and Hesse's data protection law, passed in 1970, was the first data protection law in the world.[53] Data protection, and privacy generally, generated state, national and international legislators' attention particularly in the wake of Nazism and Communism – as discussed above, but took on additional urgency in the 1960s as computerization of state data processing got underway. In Hesse too the specific motivation for legislation arose in connection with instalment of powerful mainframe computers; the "act was about differences between local communities and the state administration, about who should be allowed to buy these new machines, the large computing systems, and who should decide which programs to run on them, or rather, the act was a follow-up to the law that tried to settle these arguments."[54] It was not only the first data protection legislation, but may fairly be said to be the most influential, as subsequent federal data protection legislation, most notably Germany's Federal Data Protection Act (*Bundesdatenschutzgesetz*, "BDSG") passed in 1977, was built on the Hesse law, and BDSG in turn greatly influenced EU law. Many of the frameworks and terms, including the phrase "data protection" and the establishment of data protection commissions, owe their genesis to the Hesse law.[55] Privacy in German law is protected as a part of the rights of personality (*Persönlichkeitsrechte*), and the Basic Law of 1949 specifically safeguarded privacy as "the Germans were sensitive to their tyrannical past."[56] The Hessian law was undoubtedly influenced by the German, and Hessian, Holocaust past,[57] and more generally European data protection laws include the hidden agenda of discouraging a recurrence of Nazi and Gestapo efforts to

[51] Biedermann, "50th Anniversary", p. 454.
[52] McDonald, "Reconciling Holocaust Scholarship", p. 1360.
[53] "Hessisches Datenschutzgesetz" (The Hesse Data Protection Act), in *Gesetz und Verordungsblatt I,* 1970, p. 625.
[54] Burkert, "Privacy – Data Protection".
[55] Kosta, *Consent in European Data Protection Law*, pp. 44-45.
[56] Bennett, *Regulating Privacy*, p. 75.
[57] Flaherty, *Protecting Privacy*, p. 24; Richie, "The Role of the Epistemic", p. 139.

control the population,[58] and it and the BDSG were both legislative acts giving specific legislative protection to the personality rights protected by German and international human rights law.

The BDSG, as first passed,[59] included a blanket prohibition on the processing of personal data, save where BDSG allows it, another regulation allows it, or the data subject consents. Consent must be given in writing, and processing without obtaining consent would be illegal. BDSG avoided some of the thornier problems of definition by placing all personal data in a highly protected category, in contrast with other jurisdictions which have a separate category of sensitive personal data.[60] Section 11 of the BDSG allows transfer from the processor to a non-governmental third party where a "justified interest", meaning "any interest which the legal system recognizes as worthy of protection",[61] could be identified. The Bonn Accords presumably provide sufficient evidence that Holocaust preservation and justice are interests worthy of protection. Superficially, this avenue would not have been workable, as BDSG requires that the transferor must ensure that no person who is to be protected by the law is harmed by the release of data, and the assessments of "justified interest" must be made on a case-by-case basis. But there is precedent for just such a move: in 1998 the US Nazi War Crimes and Japanese Imperial Government Records Interagency Working Group (IWG), instructed by Congress, released over 8 million documents, each of which was reviewed for privacy violations, and tens of millions more documents were reviewed as part of the process of identifying which documents are candidates for release (the US National Archives alone reviewed 60 million documents regarding Japanese war crimes – in addition to reviews at the Department of Defense, Department of State, CIA, etc.).[62] The US Nazi War Crimes Disclosure Act[63] which governed the IWG's work includes provisions in line with Biedermann's assertions: "…the Nazi War Criminal Records Interagency Working Group shall release in their entirety Nazi war criminal records… An agency head may exempt from release… specific information, that would… constitute a clearly unwarranted invasion of personal privacy" (section 3(b)). Thus Biedermann's legal position appears to be basically coherent and legitimate, taken in isolation, and in line with other jurisdictions' treatment of Holocaust-related archival material, but the conclusion was misguided. Arolsen is estimated to have 50-100 million documents,[64] on the same order as the IWG's work. IWG has published the costs of this project, amounting to several

[58] See note 2 above.
[59] Riccardi, "The German Federal Data Protection Act of 1977".
[60] *Ibid*., p. 249.
[61] *Ibid*., p. 256.
[62] http://www.foia.cia.gov/collection/nazi-war-crimes-disclosure-act.
[63] http://www.archives.gov/about/laws/nazi-war-crimes.html.
[64] Shapiro, Foreword to S. Brown-Fleming, p. x.

$M per year, which ought not to be prohibitive for an organization financed by the German government and employing almost 300 people.

Even barring a general release pursuant to international law immunity, and a review-and-release following IWG's lead, some technical-legal solutions could have been applied more effectively to enable documents to be released. ITS required advance requests for access to information, would refuse access if it determined that the applicant could find the information elsewhere, and – amazingly – ITS required scholar applicants to pay for staff assistance and to buy indemnity insurance for ITS, the International Red Cross and the Commission's eleven governments in case a document was misused.[65] Likewise, if scholars and others cleared these hurdles, information eventually provided was subject to one final caveat: "The ICRC insisted that all information in the documents relating to persons, places, or dates be 'anonymized' – that is, blacked out."[66] Other simpler and less onerous tools could have been applied, for example, judicious use of Non-Disclosure Agreement (NDA);[67] the member governments, instead of being indemnified by researchers, ought to have indemnified ITS and the researchers or provided a general release and waiver. There could also be created, through NDAs or some other form of contractual arrangement, a mechanism broadly analogous to the Privacy Shield program;[68] this would allow researchers, restitution experts, Yad Vashem, USHMM and other interested parties the ability to make use of the archives without exposing the German government or ITS to claims by data subjects. Such a Privacy-Shield-like arrangement was made, for example, in the French banks' settlement with Holocaust victims: the Mattéoli Commission had constructed a list of 64,000 names of French Holocaust victims and 80,000 accounts they had held; the lists were not published for privacy concerns, but they were made available to Holocaust institutions and to American lawyers acting in the restitution process.[69] Additional solutions might have required pushing for legislation to be passed specifically exempting liability for privacy breaches resulting from opening the archive, or some form of court order to force compliance with the Bonn Accords.[70] Or, finally, an unlikely but available course would have been for the archives to basically flaunt BDSG, and wait to see if someone, anyone, whose privacy is harmed takes any action. This was ultimately what happened, and according to Shapiro – writing in October 2015 – in the intervening years no legal action for violation of privacy materialized.[71] To the extent that there was a true concern for the civil liability involved, the interested parties could have formed an indemnity

[65] Shapiro, "History Held Hostage", p. 42.
[66] *Ibid*.
[67] As discussed by McDonald, "Reconciling Holocaust Scholarship", p. 1386.
[68] *Ibid*., p. 1388.
[69] Eizenstat, *Imperfect Justice*, p. 328.
[70] McDonald, "Reconciling Holocaust Scholarship".
[71] Shapiro, Foreword to S. Brown-Fleming, p. xix.

fund, to indemnify ITS from any possible suits. Few organizations are culturally and legally bold enough to take such an approach – though the Holocaust Museum and Yad Vashem were.

We have seen how ITS could have pursued several avenues to release many or all documents. Missing entirely from ITS' consideration of the conundrum were the purpose and principles of data protection in German law. As shown, the stringencies of European, and especially German, privacy law are largely a reaction to the Nazi, and later Communist, regimes in Europe, and the "desire to build institutional and cultural barriers against the comprehensive monitoring of private life that appeared – before the Second World War and during the Cold War years – as a necessary condition for the functioning of totalitarian or authoritarian regimes."[72] Some have suggested that this explains Germany's and the EU's particular emphasis on "sensitive data".[73] Thus, against the backdrop of the particular stringencies of German data protection law, Biedermann's position technically makes legal sense. However, when broadening the perspective to the historical context in which, and ends to which, the archive was created, Biedermann's view represents an inordinately and indefensibly narrow approach to the relationship of privacy to the archives. A broader and more purposive approach to BDSG, in light of the circumstances of Holocaust victims and their dignity – particularly considering the survivors' ages – could have led to a very different position. Undoubtedly, the technicalities of individual rights under the BDSG would have made it very difficult indeed to follow through on opening the ITS archives without limitation, but the particulars of the circumstances ought to have led ITS to take two important positions.

One is that the vast majority of Holocaust victims would want to share their information, and would much sooner have private details of their Holocaust horrors revealed with the entire archive, than have it remain under wraps. They would rather be connected with a living relative without being asked than delay months and years before finding one. The vast majority of them have nothing to hide from their Holocaust years, their experiences – at least as documented – may evoke feelings of pain, anger, shame and so on, but few if any would ever think: "that cannot be published, it's private!"[74] Organizations representing Holocaust victims certainly considered that the case, and it was they who led the fight to open the archives. If this was presumed to be true, this might have effectively bypassed the need for a case-by-case analysis, though such a bold position may be too much to ask from a quasi-governmental institution. One may plausibly counter that the

---

[72] Bennett and Raab, *The Governance of Privacy,* pp. 18-19. See note 3 above.

[73] Winn, "Can a duty", p. 245; quoted in de Azevedo Cunha, *Market Integration,* p. 2.

[74] See below, at note 151, that this was also the experience of the Hungarian DPA: there "has been no evidence for protest on the part of those involved or their families." Anecdotally, this author has the same impression from interviewing several survivors, and hopefully those findings will be published in due course.

law must, and is indeed intended to protect the minority of data subjects who would object to their data being shared in such circumstances. Since enquiring with each data subject would not have been workable, ITS could for example have run a huge marketing campaign to ensure that all Holocaust victims are aware of the impending revelations, and could have a chance to register objections, perhaps be indemnified or even compensated, or some alternate arrangement could have been made. Though Biedermann did not specify whose privacy is concerned, and it seems that he was protective also, if not primarily, of the privacy of Nazis, and their heirs. Revelation of German Nazis could cause real embarrassment and anguish to them and their descendants, and more generally to the German public. The European Data Protection directive[75] protects only the data rights of a natural person – to the exclusion of, amongst others, legal persons, and the deceased.[76] But the privacy rights of the families of the direct, primary data subjects may be evoked such as where the families would be subjected to excessive press interest;[77] however, for ITS to allow Nazis and their families to use their privacy rights to obstruct their victims from restitution and justice is morally repugnant. The rights in question ought not to be divorced from the context of victims and perpetrators; privacy rights of the Nazis' heirs ought not to take precedence over the property rights of murdered Jews, and over the cause of justice. The ultimate capitulation of ITS seems to reflect an acceptance that – deep and painful as the stigma may be in a re-normalized Germany – the revelation of a person's Nazi past and Nazi ancestry must not be allowed to obstruct Holocaust justice and truth.

Second, ITS could have advocated for a purposive interpretation of BDSG. Privacy in Germany is a human right, derived from German law of dignity, and there are good grounds to argue that in the circumstances of ITS the victims' dignity is much better served by allowing the archives to be disseminated, serving justice and truth, than by keeping them under a cloak of privacy. This latter point needs some explanation. Some have suggested that the European privacy law is premised on dignity, basically inherited from the Roman law tradition.[78] Others have suggested that European law is premised on liberty.[79] But whether European notions of privacy

---

[75] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[76] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[77] Compare *National Archives and Records Administration v Favish* 541 U.S. 157, pp. 168-169 (2004), at US Supreme Court. See discussion in Schreiber, "Privacy: Proprietary or Human Right?", pp. 106-107.

[78] Wittmann, "The Two Western Cultures". According to Bloustein, "Privacy as an Aspect", p. 971, this is how the founders of modern privacy law – Warren and Brandeis, in "The Right to Privacy" – saw things.

[79] Bignami, "European Versus American Liberty", p. 612; see discussion, with endorsement of Bignami's view, in Solove, *Understanding Privacy,* pp. 185-6.

are generally and historically derived of concepts of dignity or liberty, at German law today privacy is certainly viewed as protecting the dignity of the subject, and case law confirms that this is protected under article 2 of the constitutional *Grundgesetz*.[80] German constitutional law, including privacy law, allowed plenty of room for balancing with other fundamental rights, and with the central constitutional value of dignity which underlies privacy itself. In a clash between victims' and perpetrators' dignity, only one outcome ought to emerge. Germany's Federal Constitutional Court has already asserted the value that German law assigns to protecting the dignity of Holocaust victims and their descendants, specifically through prohibition of Holocaust denial,[81] and one is hard pressed to imagine a situation in which the dignity (i.e. privacy) of perpetrators and their descendants could possibly trump that.

So ITS' position, under Biedermann, was perhaps technically valid, but it was extremely short-sighted, and showed a failure to appreciate the significance and purpose of German privacy law, and of the archives and their role in justice and truth, beyond addressing specific requests for information from victims. It failed to consider the purpose of privacy, and what it protects. This then is the important lesson of the ITS experience: privacy rights will generally be, and ought to be, dwarfed by the cause of justice in human rights violations, and the harm to dignity will be *de minimis* as compared with the enhancement of dignity served by revelation of the violations. Thus privacy must not be allowed to obstruct truth, justice and accountability.

Following the processes described above, ITS has digitized and transferred its archives to its eleven member states, including Israel, through Yad Vashem, and the US, through the USHMM.[82]

## Privacy as a Limitation on Justice

With respect to privacy violations, the Holocaust was the perfect storm. Technologically, it was perfectly timed for the perpetrators: the pre-computer sorting technology, and notably the punch-card Hollerith machines provided by IBM and its subsidiary Dehomag, which were the nerve centre of Holocaust camps,[83] enabled the high degree of organization and efficiency required for the effective perpetration of the Holocaust. Conversely, the pre-digital technologies and

[80] E.J. Eberle, "Human Dignity", pp. 976 and 1000. The *Grundgesetz* was passed as part of Germany's "seeking distance from the horrors of Nazism", *ibid*., p. 967.

[81] Krotoszynski Jr., "The Polysemy of Privacy", p. 908, footnotes omitted. See BVerfGE 90, 241, p.254, referring to an earlier Federal Court of Justice Case from 1979, BGHZ 75, 160. See discussion in Krotoszynski Jr. specifically with respect to privacy, and more generally Pech, *The Law of Holocaust Denial*.

[82] http://www.yadvashem.org/yv/en/about/archive/new_its.asp#!prettyPhoto.

[83] Black, *IBM and the Holocaust*, p. 351.

evidence were hard to copy and easy to destroy, leading to enormous difficulties in providing admissible evidence for atrocities. Thus the Germans used the data-rich environment they created to perpetrate the atrocities of the Holocaust, and then exploited the weaknesses of the technology to destroy evidence.

Generally, the crimes of the Holocaust were characterized by a systematic cover-up, as those who witnessed the atrocities were, overwhelmingly, killed.[84] The first Auschwitz Trials were at Poland's Supreme National Tribunal, including the trial of Rudolf Höss in Warsaw in March 1947; another forty-one staff were tried in Kraków later that year, leading to convictions, including death sentences. The Frankfurt-Auschwitz Trials in 1963-1965, tried under German law, led to various convictions from among the twenty-two defendants, mostly as accessories to murder, though several were acquitted. Others were tried in various jurisdictions, but probably not even 10%, and certainly not more than 15%, of approximately 7,000 – 7,200 SS staff that served at Auschwitz were ever tried,[85] much less convicted or punished.

Aside from the considerable legal and political challenges involved, the systematic cover-up and destruction of evidence have made the Holocaust criminals that much harder to bring to justice. A commandant of Auschwitz, Rudolf Höss wrote – explaining why it was impossible after the war to arrive at a reasonably accurate number of victims at Auschwitz – that:

> "…after every large action all evidence in Auschwitz on which a calculation of the number of victims could be based had to be burnt… I personally destroyed every bit of evidence which could be found in my office… Reichsführer SS and the Reich Security Head Office also had all their data destroyed."[86]

Thus, technology was at such a stage as to facilitate efficient killing through the use of data processing, teleprinters and wireless, but not yet sufficiently developed to enable easy copying, conservation and sharing. This was just one of several factors making Holocaust justice so hard to exact. But in some instances it had a decisive influence on the failure of justice. For example, the case of Belzec is instructive. At Belzec 600,000 Jews were murdered, and only two survived: Chaim Hirszman was killed in 1946, and Rudolf Reder testified in the Belzec Trial in Munich in 1965,[87] and died shortly thereafter, in 1968, at the age of 87. Only SS

---

[84] Once they understood that they would be tried as war criminals, leading Holocaust murderers accelerated the murder of the Jews and destruction of evidence; Hans Frank, director of the General Government in Poland, famously told his subordinates as much on January 25, 1943, and recorded this in his diary. See McKale, *Nazis After Hitler*, pp. 157-8.

[85] Lasik, *Historical-Sociological Profile*, p. 282; and Lasik, *Postwar Prosecution*, p. 588 *et seq*.

[86] Höss, *Commandant of Auschwitz*, p. 193.

[87] http://www.holocaust-history.org/german-trials/belzec-urteil.shtml.

officer Josef Oberhauser was convicted, while others were quickly acquitted, and Oberhauser himself was convicted only of various forms of accessory to murder.[88] Thus, half a century ago – by the late 1960s – there was little hope of ever bringing to justice any of the murderers of Belzec.[89] There were very few instances of justice being done with Holocaust protagonists, yet when the few opportunities arose, there emerged an additional important legal barrier to justice, namely the privacy of the accused. For example, at the Frankfurt-Auschwitz Trials, Hesse Attorney-General Fritz Bauer[90] and "the prosecution made tremendous efforts – not always successful, unfortunately – to overcome the limitations of the law and to use the trial for didactic purposes" but, in "accordance with German privacy laws, the indictment has remained unpublished to this day."[91] In the meantime, the indictments have been published, as were the verdicts, and as detailed by Pendas and Wittmann there was considerable press coverage of the trials, to the point that the "public discussion of the crimes at Auschwitz did run counter to normal standards of confidentiality and defendants' rights in a criminal trial held under the West German penal code."[92] The indictments were considered private since the allegations were as yet unproven, and the early publications of the trials anonymized the witnesses and defendants.[93] Privacy here may be viewed as masking a much more deep-seated issue: by some accounts, "a pathological abreaction to the trauma of having perpetrated the greatest crime in human history."[94] Privacy rights of Auschwitz murderers thus prevented their trials from furthering truth and justice, even if their abuse in this way was masking deep-seated psychological needs of the German public.

This affords us an opportunity to consider the role of anonymization in Holocaust justice and research. Anonymization/pseudonymization was applied to the indictments at the Frankfurt-Auschwitz Trials,[95] and similarly has been

---

[88] It is beyond the rubric of this article, but some peculiarities of German criminal law and its interpretation throughout the second half of the twentieth century meant that overwhelmingly the worst conviction possible for a Nazi was accessory to murder; see discussion in Wittmann, *Beyond Justice*, p. 36 *et seq*.; Bennet, "The Limits", p. 126.

[89] Some were convicted for crimes committed elsewhere, especially at Sobibor. For details, see Bryant, *Eyewitness to Genocide* (2014), whose general conclusions have not persuaded this author.

[90] Bauer was born to Jewish parents, was himself briefly interred in a concentration camp as a vocal opponent of the Nazis, and was instrumental in the Eichmann capture.

[91] Pendas, "I didn't know", p. 445 and fn. 155, footnote omitted.

[92] Wittmann, *Beyond Justice* (n. 87), p. 206.

[93] Pendas, by personal communication.

[94] Pendas, "I didn't know", p. 405.

[95] It is beyond the rubric of this article, but deserves mention, that anonymization was also applied in Israeli Kapo police files. In the early 1990s, the Israeli Police determined that the remaining Kapo files be sealed for seventy years from the date each file was opened, mostly in the early 1950s. In 2015, Israeli news site News1 and its legal correspondent, Holocaust researcher Itamar Levin, succeeded in having most of those files opened. In total, fifty-three files were opened; see Levin (n.68), p. 21. These were not, as suggested by O. Ben-Naftali and Y. Tuval, "Punishing International Crimes", 150-1, court rulings, but police files, and the sealing order was not for seventy years from

used in historical research. For example, in conducting research for "Ordinary Men', Christopher Browning was granted access to Court of Hamburg records, specifically for Reserve Police Battalion 101, which was the focus of his study. He was however required to undertake not to use the men's real names, but to pseudonymize the data. In Browning's words:

> "Regulations and law for the protection of privacy have become increasingly restrictive in Germany… I had to promise not to use the men's real names… While this promise of confidentiality and use of pseudonyms is, in my opinion, an unfortunate limitation on strict historical accuracy, I do not believe it undermines the integrity or primary usefulness of this study."[96]

As Browning notes, for the purposes of his study and thesis, pseudonymization was not too problematic, though plainly pseudonymization or anonymization makes it at least more difficult to verify and corroborate, refute and develop historical analysis. Likewise, publication of anonymized indictments, or law enforcement or historical research would significantly undermine their impact. Ironically, again, anonymization and pseudonymization were yet another important German contribution to European privacy law inspired or educated by Holocaust-era atrocities; as Reidenberg wrote, "the modern German history of the Holocaust offers a compelling motive to promote anonymity",[97] and pseudonymization and anonymization have now become integral to European privacy law,[98] but they have frequently been applied to the detriment of Holocaust education and healing.

Though pseudonymization and anonymization were not necessarily debilitating to Browning, in the case of ITS they seem to have been prohibitive: Browning was provided information and he himself pseudonymized it. ITS would actually anonymize information provided to researchers, impairing the research and confounding both ITS' and the researchers' objectives. Likewise, whereas Browning's research was focused on perpetrators, the same anonymization when applied to victims greatly undermines the research. The frustration of a researcher

---

the date of the judgment, but for seventy years from the date each police file was created; for further criticism of their paper, see Levin, *Kapo in Tel Aviv,* 19. See also Singer, "Reductio Ad Absurdum", citing Cassese, *The Oxford Companion*, p. 696. Privacy was a central concern, and Levin was able to get the files opened for his research on condition that the privacy of the families be preserved; specifically he agreed to pseudonymize individuals' identities, using initials, in his publication (Personal communication from Levin, March 22, 2016).

[96] Browning, *Ordinary Men*, pp. xx-xxi.

[97] Reidenberg, "Resolving Conflicting", p. 1350.

[98] GDPR Article 6(3a)(e) introduces pseudonymization as a consideration in allowing processing of personal data other than for a purpose for which it was collected, preceded by Article 29 Data Protection Working Party's "Opinion 05/2014 on Anonymisation Techniques". For critique of anonymization as a privacy tool, see Ohm, "Broken Promises".

of victims of Nazi medical experimentation, Weindling, writing in 2014, is worth quoting at length:

> "Certain German archives have imposed far-reaching anonymization restrictions, notably the German Federal Archives requiring complete anonymization, and destruction of notes and the secure database entries on completion of the research. This condition is despite the fact that reconstructing a life history involves linkage from several sources, so that the database constitutes a unique record of a person's odyssey through camps and clinics, otherwise hidden from history… Anonymization of victims of systemized violence and murder, many deceased for over fifty years raises significant issues. These include why there are severe legal sanctions to publishing in ways restoring identity of persons who were persecuted and consigned to oblivion, and reconstructing the abuses to which victims were subjected? Names are essential for the cohort analysis, in order to link records and to ensure there is no double counting. Naming a victim is to restore identity and a whole sense of the historic person to individuals reduced to being camp numbers and research material…"[99]

Weindling raises several problematic aspects of anonymization, and notes the need to ultimately name all murdered and mutilated victims. His conviction is shared by the Holocaust research and memorialisation movement which seeks to name all the victims of the Holocaust. But beyond the softer form of injustice in perpetuating the Nazi de-identification of victims, anonymization crimps some more tangible forms of justice. To appreciate just how grave an injustice occurs when the mechanics of justice are shrouded in privacy, we may look to a Holocaust trial from the same period as the Frankfurt-Auschwitz Trials that made enormous contributions to Holocaust justice, particularly because it was so public. The case that added a sense of urgency and vogue[100] to Holocaust justice and research was one of the most famous cases in history: the trial[101] – and subsequent execution – of Adolf Eichmann, under Israel's Justice for Nazis Law. Eichmann claimed that that law could not be applied to him for acts committed before the law was passed, outside the state of Israel, and against people who were not citizens of the State of Israel. The court had no technical rebuttal of these apparently sound claims, and rested instead on the injustice and immorality underlying his procedural claims, and the repugnance of a failure of justice in the face of such odious crimes based on the fact that the requisite laws were not in effect at the time.[102] The Israeli court, like the IMT before it, appealed to "universal moral values', and its outrage at the

[99] Weindling, *Victims and Survivors*, pp. xvi-xvii.
[100] Cohen, *Israeli Holocaust Research*, p. 190 *et seq*.
[101] Criminal Appeal 336/61 *Adolf Eichmann v. Attorney General*, PD 16:2033 (1961).
[102] *Eichmann* (n.102), para. 8.

violation of those values overwhelmed otherwise sound procedural-legal claims. This same outrage – completely missing from the Auschwitz-Frankfurt Trials, and indeed all early German Holocaust trials,[103] – ought to have led the court to quickly brush aside any privacy considerations for self-confessed Auschwitz SS staff.

This is not a novel suggestion. It was, for example, the policy of the Allies at the conclusion of the Second World War, when various sites of atrocities were revealed and photographed. The United States Supreme Court has rightly noted that it was the policy of the US government to disseminate these images precisely because the invasions of privacy in such instances are *de minimis* in and of themselves, and are insignificant in light of the purpose served, meaning they must be trumped by the need for accountability of perpetrators:

> "At the end of the [Second World] war, the United States government widely disseminated photographs of prisoners in Japanese and German prison and concentration camps… These photographs of emaciated prisoners, corpses, and remains of prisoners depicted detainees in states of powerlessness and subjugation… the United States championed the use and dissemination of such photographs to hold perpetrators accountable."[104]

Thus the principle that justice for Holocaust victims ought not to be obstructed by claims of their privacy was established – if not by declared principle, then by practice – immediately upon the discovery of the horrors of the Holocaust. More generally, the need for and value of publicity in Holocaust justice is demonstrable. The trial of Adolf Eichmann was by far the most influential of all Holocaust trials after IMT; it had major ramifications internationally, for several reasons. These include the drama and intrigue surrounding Eichmann's capture;[105] and the symbolism of his trial at the hands of his main victims, the Jews, also enhanced the effects of the trial.[106] But of all the factors contributing to the fame and impact

---

[103] Indeed, one distinguishing feature of the Frankfurt Trials – in contrast with IMT and *Eichmann* – is that they were prosecutions under ordinary German criminal law, and therefore the SS staff were rather logically granted ordinary privacy protection. The extraordinary legal premises of the IMT and *Eichmann* meant that certain technical-procedural claims were effectively disregarded. More generally, the German judiciary was very largely implicated in Nazism, and: "Few professional groups in German society were as implicated in the Third Reich's misdeeds as lawyers and judges." Bryant (n.93), p. 12. As a result, "many were reluctant to pursue Nazi crimes vigorously, given their own far from unimpeachable professional biographies." Pendas, *The Frankfurt Auschwitz Trial*, p. 13. Generally, and for well-documented reasons, Germans trying Germans generally showed little enthusiasm for these trials. Cf. Bryant, *Eyewitness to Genocide*.

[104] *American Civil Liberties Union v. Department of Defense* 543 F.3d 59 (2008), p. 89.

[105] His capture and surreptitious extradition to Israel were specifically discussed and condemned at the UN Security Council: UN Security Council Resolution 138 (1960).

[106] The trial effected a revolution in arresting and even reversing twenty years of Israeli apathy and even hostility toward Holocaust survivors and victims: Yablonka, "Justice for Nazis", p. 149; Stern, "Judgment in the Shadow", p. 427.

of the case, the greatest – itself partially an outcome of the previous factors – seems to be the publicity given to individual victims and their stories, and to the trial generally. The trial was one of the first to be televised, and in Israel – where television was introduced only seven years later – it was radio-broadcast live.[107] It was broadcast over four months, in 56 countries. By some accounts, eighty percent of German adults watched the trial.[108] As a result, the Eichmann capture and trial "had a profound impact on West Germany, which initiated the first serious steps to bring those implicated in the Nazi mass murder to trial… The Eichmann judgment was a catalyst for ushering in an age of global justice devoted to the development of an international jurisprudence dedicated to the punishment of severe and serious international offenses."[109] The Eichmann trial was embarrassing for the Austrian, German and other governments that knew, or could easily have known, of his whereabouts and did nothing about it,[110] and apparently spurred many to at least be seen to be making an effort. For example, shortly after the Eichmann trial and in reaction to it, Franz Stangl, Austrian-born commandant of Sobibor and Treblinka, was found in Brazil, where he was working for a German company with Nazi roots – Volkswagen – under his own name. He was extradited to West Germany, tried and convicted, sentenced to life in prison, and died shortly thereafter of heart failure.[111] These processes catalysed by the Eichmann trial underscore the importance and value of justice being done publically, and the dangers of privacy curbing justice.

Tragically, in Germany and elsewhere privacy was a formidable barrier to Holocaust justice, and that started to change only once it was too late to have a material impact. Holocaust justice for Nazis is now in its pathetic closing act. The 2011 conviction[112] of John Demjanjuk in Munich, on the basis that he served as a guard in Treblinka, set a new and important precedent in German criminal law – basically making an accessory to murder anyone who was part of the camp staff, without having to prove involvement in the murder of a specific individual – and this enabled additional Holocaust cases to be pursued.[113] In 2013, German prosecutors were reported to have a list of fifty guards from Auschwitz still alive in Germany,[114] but this has led to only a handful of indictments and fewer convictions.

---

[107] See at length Pinchevski *et al.*, "Eichmann on the Air".

[108] http://www.haaretz.com/jewish-world/jewish-world-news/.premium-1.638191.

[109] Lippman, "Genocide", pp. 66 and 121, footnote omitted.

[110] And later for the US government, since it was revealed, pursuant to the Nazi War Crimes Disclosure Act, that the CIA had long known of Eichmann's whereabouts. See Lichtblau, *The Nazis Next Door*, p. 70; Naftali, *The CIA*, pp. 337-374.

[111] McKale, *Nazis After Hitler,* pp. 297-307.

[112] He died before his appeal was ruled on, so, technically, he died presumed innocent.

[113] See note 90 above.

[114] http://www.spiegel.de/international/germany/german-prosecutors-to-investigate-50-former-auschwitz-guards-a-893123.html.

Oskar Gröning was a bookkeeper at Auschwitz, charged with counting, sorting and guarding the money and valuables looted from the murdered Jews, though from his very first day there he was aware that he was part of the mass murder of Jews. In 2015, at the age of 93, Gröning was convicted of being an accessory to murder, and was sentenced to four years in prison. In June 2016, former Auschwitz SS guard Reinhold Hanning was convicted and sentenced to five years in prison. He died in May 2017 before exhausting his appeal. A case for accessory to 3,681 murders against Auschwitz accountant Hubert Zafke was ended in August 2017 on account of his dementia making him unfit to stand trial. These are likely the last Holocaust Nazis to stand trial, in some form, and the change led by the Demjanjuk case came over half a century too late for the Frankfurt-Auschwitz Trials, and altogether too late for a chance to have a meaningful impact.

In the meantime, in one specific case, the matter of Holocaust justice was pitted directly against the right to privacy. Heinrich Boere was a Dutch-German Waffen-SS volunteer, who murdered several Dutchmen in cold blood during the war. He was arrested after the war, and subsequently released, but after a few years in hiding in Holland he proceeded to live out his life in peace in Germany, though he was sentenced *in absentia* in Holland. In 2008 the prosecutor in Dortmund filed charges against him, and in 2010 he was convicted and imprisoned, dying while serving the sentence in 2013. In the period after his charging and before his trial commenced, Jelle Visser and Jan Ponsen, two Dutch journalists, sought to interview him, contacting Boere's lawyer and family. Eventually, in 2009, they simply drove to his old age home in Germany, interviewed him[115] there, and surreptitiously filmed and then published the interview. The footage included what amounts to a confession by Boere of the murders, particularly notable given that he had thereto denied the charges. The local prosecutor in Germany promptly filed charges against the two journalists for criminal invasion of privacy.[116] In their case, their judge ruled that the revelations were in the public interest and that the information – Boere's confession – would not have been available but for their actions, and as such found them innocent of criminal invasion of privacy.

In summary, only a very small proportion of Holocaust perpetrators were ever tried, only a fraction of those were convicted and given meaningful sentences. One of the many obstacles to justice was privacy – which was allowed to curb the crucial ripple effects of justice: this greatly limited the drama and publicity of the court proceedings; there was limited stigmatization, limited warning to others, which eclipsed the healing for victims and ameliorated the educational value of the trials. The role of privacy in blocking Holocaust justice reflected a lack of outrage, a legal and moral position in which being a camp guard at Treblinka and

[115] Visser here tells the story in detail: https://thelede.blogs.nytimes.com/2012/02/07/dutch-reporters-face-trial-in-germany-accused-of-violating-nazi-war-criminals-privacy/?_r=0.
[116] 1 Js 417/09.

methodically killing thousands was, at worst, accessory to murder. These Holocaust cases ran afoul of the notion "that justice should not only be done, but should manifestly and undoubtedly be seen to be done."[117] Indeed, in not being manifestly seen to be done, justice was not actually done. Though the opportunities for justice for Nazis are now all but irretrievably gone, there are still some secondary forms of justice that must continue to be done, and there too privacy has proven to be a significant barrier. The same is true of Holocaust research, which has likewise been eclipsed by privacy considerations. As demonstrated in the next section, privacy rights have been systematically used to obstruct one of the areas in which justice can be done with victims' progeny – Holocaust property restitution.

## Post-Holocaust Restitution and Privacy

Financial institutions, principally banks and insurers, have for decades been wrangling with privacy issues in the US, Europe and Israel, to the detriment of Holocaust victims. In this section a few examples are discussed so as to provide a sample of injustices in property restitution perpetrated or perpetuated by reference to privacy.

In 1998 the International Commission on Holocaust Era Insurance Claims (ICHEIC, pronounced "eye-check") was established, and by March 2007 ICHEIC had resolved over 90,000 claims, distributed over US$306 million to over 48,000 Holocaust survivors or heirs.[118] This was not without considerable obstacles and challenges along the way,[119] one of which – as noted by ICHEIC's chairman – was that ICHEIC "had to reach agreement on the publication of lists of potential claimants when European privacy laws often stand in the way of our broadcasting those names."[120] ICHEIC instituted some novel procedural steps to accelerate the process. Most notably, "[r]elaxed standards of proof[121] were adopted by ICHEIC to ensure thorough investigation by the companies of every claim regardless of the kind of evidence submitted and serious assessment of "the strength and plausibility of non-documentary or unofficial documentary evidence".[122] Where the claimant could prove the existence of a policy, the burden shifted to the company to demonstrate the policy's status. It was up to insurer to show an adjustment of

---

[117] *R v. Sussex Justices, Ex parte McCarthy,* [1924] 1 KB 256, per Lord Hewart CJ.
[118] http://www.icheic.org/about.html.
[119] See at length Zabludoff, *ICHEIC*, p. 260 *et seq.*
[120] A letter from ICHEIC Chairman Eagleburger to forty-five congressional representatives, October 11, 2000; cited in Bazyler, *Holocaust Justice,* p. 166.
[121] ICHEIC, Standards of Proof (15 July 1999), available at: http://www.icheic.org/pdf/ICHEIC_SP.pdf; see also Trilateral Agreement (note 59), at Annex B.
[122] ICHEIC Holocaust Era Insurance Claims Processing Guide 8 (1st Edition, 22 June 2003), p. 20, available at: http://www.icheic.org/pdf/ICHEIC_CPG.pdf.

the policy's value or its previous payment."[123] With relaxed rules of evidence, the insurance companies mounted an enormous obstacle by refusing to publish the lists of wartime policyholders, so that the evidentiary stage could not really get off the ground. This was in most cases an insurmountable hurdle since the majority of the policy beneficiaries were altogether unaware of the policies or unable to prove their existence; many had been children, and few had documentary evidence of policies. To be clear, here too the claims of privacy consideration were disingenuous; European insurers could have bypassed this obstacle, as the Swiss banks had done,[124] and as Dutch insurers, and Allianz – a German insurer – had agreed to make its list of pre-war policyholders public, subject to various restrictions. Nonetheless, European insurance companies stalled rather successfully, and persisted with the claim that policyholders' privacy cannot be jeopardized.[125]

The insurers were very successful in avoiding paying out on insurance claims of Holocaust victims, and ICHEIC really achieved very little restitution. The same is true for the German Slave Labour litigation, which ultimately resulted in an average of just US$5,000 per labourer/slave. But the data collected during the process made a unique and lasting contribution to Holocaust studies. A prominent lawyer in the US bank and insurance restitution cases wrote that one of the major justifications for the cases, at least in retrospect, was "to build a historical record that could never be denied",[126] such as "the 580,000 questionnaires returned in the Swiss bank case… the last and only poll of the surviving Holocaust generation." The most important contribution of these cases, like that of the Eichmann case and the ICHEIC process, was arguably in the contributions it made to history and memory, and in particular to re-individualization of the victims and their healing.[127] Yet the failures of restitution processes and the pivotal and negative role privacy law played in those processes must not be overlooked.[128]

Sadly and ironically, Israeli banks have been even less cooperative than Swiss banks, and folded on their faux privacy principles much later than the Swiss banks, when even fewer survivors were still alive. The Israeli Knesset conducted

---

[123] Less, "International Administration", p. 1668.

[124] The extensive publicity of the Swiss Banks saga also helped break down resistance of others: "The Swiss restitution experience had taught the Dutch government… that legal arguments in such negotiations are sometimes secondary. They had also shown that moral aspects can become dominant if the media and public opinion treat them as such." Gerstenfeld, *Judging the Netherlands*, p. 18.

[125] Bazyler, *Holocaust Justice,* p. 151 *et seq*., re: insurers and banks using privacy as excuse for non-revelation.

[126] Neuborne, "Preliminary Reflections".

[127] Less, "International Administration", p. 1692.

[128] Germany's Federal Data Protection Authority specifically managed data protection aspects of ICHEIC. See Bundesbeauftragten für den Datenschutz report for 2001-2002, p. 50: https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/19TB_01_02.pdf?__blob=publicationFile&v=7.

a parliamentary investigation[129] into the status of assets of Holocaust victims taken over by banks and the state. In the summary meeting of the committee, its chair, MK Collette Avital – now no longer an MK but since appointed chair of the Center (sic) Organizations of Holocaust Survivors in Israel – said that "in an extraordinary way, the banks consented for the first time to an external audit, despite the matter known as 'bank secrecy'. This obligated them, but also obligated us, to secrecy. And they opened all their books to us, those which they had, and funded the investigation."[130] This statement makes the Israeli banks sound very cooperative indeed, but must be read against the backdrop of decades over which Israeli banks appear to have knowingly used capital deposited by Holocaust victims in the pre-war years, while avoiding restitution to victims and their heirs. Avital herself had been Israeli Consul General in New York during the 1990s battle for restitution of Holocaust victims' assets from Swiss banks, and that experience led her to spearhead the fight for restitution from Israeli banks.[131] Specifically, Bank Leumi, formerly known as Anglo-Palestine Bank Corporation, was the main bank for the Jewish community in pre-war Palestine. Leumi, and other banks, held thousands of accounts of Holocaust victims, with sums totalling around 1 billion 2015 shekels (US$250 million); most of that had been transferred to the British Mandate – as property of enemy citizens – and thereafter assumed by the State of Israel, but held at the bank. Leumi and the other banks had been grossly deficient in interest and dividend payments, and in addition an auditor found 180 accounts of actual Holocaust victims that the bank continued to hold,[132] as well as stock portfolios and safety deposit boxes, without restitution to the rightful owners. The Knesset Committee ultimately found that Bank Leumi was liable for at least 35 million shekels of Holocaust victims' assets, excluding the majority of the sum above, which was owed by the State.[133] An Israeli law was passed in 2006 requiring organizations that hold Holocaust victims' assets to proactively seek out survivors and heirs and return their property, with provisions for inflation adjustment and interest.[134] The main case against the Israeli banks, including Leumi, was settled in 2011, for a measly 130 million shekels (US$37 million in 2011). Leumi's announcement notes that the arbitrated settlement did not mean recognition of any

[129] http://www.knesset.gov.il/protocols/search.asp?vaada=31.
[130] http://www.knesset.gov.il/protocols/data/rtf/shoa/2005-01-18.rtf.
[131] http://www.bloomberg.com/news/articles/2015-05-13/israel-restores-holocaust-assets-to-survivors-65-years-later.
[132] Amazingly, someone surreptitiously changed the language in the final draft before printing to suggest that these accounts might not be of Holocaust victims; the change was discovered in the eleventh hour and corrected: http://news.walla.co.il/item/657634.
[133] The full report, published in December 2004, is available here: https://www.knesset.gov.il/committees/heb/docs/shoa_account/shoa_finalreport.pdf. The accountants' report for Bank Leumi: https://www.knesset.gov.il/committees/heb/docs/shoa_account/shoa-app_1.pdf.
[134] The Assets of Holocaust Victims Law (Restitution to Heirs and Dedication to Aid and Commemoration) p. 5766-2006.

liability or of any claim,[135] a sad continued resistance to acknowledging its role in the injustices that may also prevent Leumi from restoring its reputation in this regard. Leumi is seen as complicit, a willing beneficiary of Holocaust crimes, and it is not surprising that it too is therefore not attaining closure, with additional suits being filed since for related restitution. The bank's avoidance of responsibility and moral and legal culpability may eventually carry a material cost.

Aside from the moral aspects of the case, at a purely utilitarian plain, Leumi could and should have learnt from the epic Swiss banks process that started in earnest in the mid-late 1990s. In the US case of *In re Holocaust Victim Assets Lit.*,[136] the court leaned on the Bergier Report[137] to detail at length the Swiss banks' use of bank secrecy as a shield from liability: "It is important to reiterate that the Swiss banks' devotion to secrecy and their repeated acts of stonewalling were not based on principles – they were profit driven."[138] The Swiss banks were quicker than the Israeli ones to recognize their roles in perpetuating injustice – to be clear, they had much more to lose as New York City initiated sanctions against UBS, Credit Suisse and Swiss Bank Corporation[139] – and in ending the spurious claims of privacy or bank secrecy used as a mask for immoral and illegal failure to make proper restitution of Holocaust victims' property. Israeli banks finally got to making some restitution, but by then it was too late to make a difference; the survivors had mostly died, and the restitution, when it was made, was generally pennies on the dollar. More importantly perhaps, it was done in a half-hearted and indignant way that denies the victims recognition, closure, and healing.[140]

However, it is not too late to recognize injustices and victims, to give them a voice, to contribute to healing. The Eichmann trial, as discussed above, had a huge impact not only in the hunt for Nazis, but in awareness of the needs of victims – survivors and the murdered, including their families, communities – and the value of memorialisation. The State of Israel's answer to the need for history, truth and memory was ultimately served more by Israel's Yad Vashem Law, than by the Justice for Nazis Law. Only one Nazi German – Eichmann[141] – was ever convicted and punished under the Justice for Nazis Law; hardly the statistics of success. By contrast, section 2 of the Yad Vashem Law authorizes Yad Vashem "to collect,

---

[135] Bank Leumi announcement, March 27, 2011: http://www.leumi.co.il/Articles/19242/.
[136] 319 F. Supp. 2d 301 (E.D.N.Y. 2004).
[137] Bergier *et al*., "Final Report".
[138] *Ibid*., p. 313.
[139] See at length Bazyler, *Holocaust Justice*, chapter 1.
[140] A recent contrast is the French state rail company SNCF. In November 2015, France agreed to pay US$ 60 million to non-French victims of the Holocaust for SNCF's role in transporting them against their will, for which SNCF was paid on a per passenger, per kilometer basis. SNCF expressed "profound sorrow and regret" for its Holocaust complicity, though not before its commercial activity in the US was threatened by Holocaust litigation: http://www.bbc.com/news/world-europe-30351196.
[141] Several Jews were tried for collaboration, as was Demjanjuk mentioned above, and Baniak – a Christian Slovak; see Yablonka, "Justice for Nazis".

examine and publish testimony of the disaster and the heroism it called forth, and to bring home its lesson to the people",[142] and it has certainly done so with great effect. In 2004 Yad Vashem made available online its Database of Names, which currently includes over 4.5 million names of Jewish Holocaust victims.[143] The State of Israel seems ultimately to have invested many more resources in implementing the Yad Vashem Law than in the Justice for Nazis Law. More resources have gone to supporting memory and healing than to justice; certainly, once the Eichmann trial catalysed various important processes of awareness and healing, the focus shifted from justice against Nazis to memorialisation and restitution.

This very abbreviated examination of Holocaust property restitution shows that privacy was, for many decades, a major obstacle to effective restitution. Though some notable settlements were made, in many cases their real contribution to Holocaust victims lay not in the restored property rights, but in advancing the memorialisation of Holocaust experiences and victims. Privacy then has effectively been utilized as a means for deferring restitution to a point where it is ineffective, perpetuating and exacerbating injustices. With the passing decades, the measure of transparency that enabled restitution of sorts ultimately made a greater contribution to memory and healing than to property restoration. This then is another conclusion that can be applied in other genocide and mass human rights violations: privacy must not be allowed to block restitution of property rights, and the passage of time will undermine restitution efforts. For restitution to be effective, it must be prompt and transparent.

## Holocaust Archiving and Data Protection

In the UK, the Information Commissioner's Officer ("ICO") had a chance to broach data protection in Holocaust research, but sadly did not choose to do so. In 2014 the government-appointed Holocaust Commission ran a public call for evidence as part of a plan of Holocaust memorialisation and education. 2,500 responses were received, and the Cabinet Office was then asked to make the material available to the public pursuant to the Freedom of Information Act. The Cabinet Office responded that the information was exempted from FOIA publication on four bases: s36(2)(b) – effective conduct of public affairs; s38(1)(b) – safety of an individual; s40(2) – personal data; and s41(1) – information provided in confidence. The ICO was of the view that section 36(2) applied, and

[142] Yad Vashem's unofficial translation, http://www.yadvashem.org/yv/en/about/pdf/YV_law.pdf.
[143] In truth, the number is significantly smaller. Yad Vashem counts every file opened, though for a very large proportion of the victims several files were opened, and Yad Vashem does not consolidate them.

apparently for that reason it unfortunately did not go on to consider the additional, alternate, bases for rejecting the FOIA request.[144]

As discussed above, ICHEIC and other processes were largely obstructed by data protection law and data protection authorities. In some cases, the national data protection authorities provided the authorization for blanket rejections of data revelation. For example, in 1999 the Florida subsidiary of a Dutch insurance company "was commanded to produce within a period of sixty days all files, records and insurance policies kept or issued by your company, its predecessors and/or its subsidiaries in the Nazi territories in the period 1940-1945." The parent company turned to the Dutch data protection authority for a ruling, and that letter responded unequivocally: "in the light of the provisions of both the Dutch Data Protection Act (WPR) and the European Directive, we see no ground which could allow you to make this extensive amount of personal data available to your American subsidiary for transmission to the American authorities."[145] Yet the Dutch DPA need not have been quite so unequivocal. As discussed throughout this article, when examining the role of data protection in Holocaust archiving, two values come into conflict. On the one hand, Holocaust research in its many forms is an expression of the "Duty to Remember" – a moral imperative to learn from history and avoid repeating it at its worst. On the other hand is European Data Protection law, premised on every person's right to control and protect their personal information. In the meeting of Holocaust archiving with Data Protection, we need to navigate the clash between these two values. As suggested above, since data protection law is premised on *dignitas*, the clash is a superficial technical one, not one of values. The clash, in so far as there is or was one, lies in the tortured souls of the survivors. This clash was at the heart of Elie Wiesel's Nobel Prize Lecture in 1986:

> "How are we to reconcile our supreme duty towards memory with the need to forget that is essential to life? No generation has had to confront this paradox with such urgency. The survivors wanted to communicate everything to the living: the victim's solitude and sorrow, the tears of mothers driven to madness, the prayers of the doomed beneath a fiery sky."

Insurance companies may use data protection laws at their convenience, but it is not their data that is being protected, it is that of Holocaust victims whose true needs were obvious even then. Thus, in 1999 the Dutch DPA was quick to see value only in data protection, but just the year before, in 1998, the Hungarian DPA was asked to opine on the transfer of microfilms of Holocaust-related trial and non-trial data from Hungarian archives to Yad Vashem, and the DPA used this opportunity to present the clash of values discussed here, and to introduce significant nuance into

[144] https://ico.org.uk/media/action-weve-taken/decision-notices/2016/1624749/fs_50585445.pdf.
[145] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z1999-0912.pdf.

the debate.[146] In that case, it was made clear that anonymization would defeat the purpose of the transfer.[147] The DPA considered best-practice among archives, and various provisions of the law, noting that archives have been sharing Holocaust-related documents freely, and there "has been no evidence for protest on the part of those involved or their families."[148] The DPA's opinion makes it clear that the data contained sensitive personal information of victims and of perpetrators and of others. Notably the DPA views the question as one of weighing collective rights, "that of collective identity and of preserving written memory of peoples", on the one hand, against "self-determination of individuals, and especially… of the victims of persecution."[149] This DPA opinion is unique in its principled consideration of the conflicting values in question, ultimately finding thus:

> "A great number of researchers and institutions agree that uncovering and disseminating the facts of the Holocaust is a historical obligation. However, exposing the facts may not result in ignoring the personal rights of the victims and potential survivors, or in the disclosure or universal accessibility of their data."[150]

The DPA here appears to exclude the personal rights of the perpetrators, but later in the opinion these are specifically included with the victims, and in particular their right to object is to be respected. The DPA proposed bi-lateral international agreement to resolve this matter, and in the meantime proposed allowing an opt-out consent to this processing, made known by a general advertisement – since contacting each data subject is impossible. The controller may need to compile a list of people with a right to object, but that list itself would be pseudonymized, and kept only for a year.

The Hungarian DPA here produced a refreshingly balanced opinion that considers not only data protection, but the meaning and value of the data in question and its processing. Rather than brushing aside Holocaust memory as an amorphous concept not protected by law, the DPA has given consideration and weight to the value underlying Holocaust memory and to the values protected by it. Holocaust archives are essential for continued research, education and restitution. In the words of Terry Cook: "Archivists are agents in constructing social and historical memory."[151] Archivists facilitating online access of archives are, in effect, making our social and historical memory accessible. Rather than our collective memories being suppressed in an archive somewhere, we seek to make

---

[146] http://osaarchivum.org/publications/accessandprotection/.
[147] Section II.8.
[148] Section IV.6.
[149] Section VI.1.
[150] Section VI.4.
[151] Cook, *Remembering the Future*, pp. 169-170.

them accessible, recallable, available. It is there that they can most contribute to healing, to research and to education. The Hungarian DPA opinion was issued with consideration to the current EU data protection directive; in May 2018 the EU's new data protection regulation, the "General Data Protection Regulation" (GDPR), becomes applicable, and its predecessor, Directive 95/46/EC, will be repealed. The new GDPR implements dramatically stricter rules of data protection, data subject rights, and much more, and can lead to hefty fines of the higher of up to four percent of global revenue or €20M. These are draconian penalties and they reflect the seriousness with which the EU has come to view data protection.

Article 83 of the 2012 draft of GDPR stated that personal data may be processed for historical research purposes, only if anonymized or pseudonymized data will not suffice. It further allowed publication of research findings only on one of three bases: (i) data subject consent; (ii) publication is necessary and the data subjects rights are not overridden; and (iii) the data subject has already made the data public. It also failed to stipulate who determines what qualifies as "historical", it did not clarify whether the restrictions will apply retroactively, and it set a very high bar to archiving and publication. This left the Stockholm Declaration (2000)[152] signatories – twenty-four of whom are EU members – in a bind, as their obligations under the Stockholm Declaration to facilitate Holocaust research appear to be in conflict with GDPR. The International Holocaust Remembrance Alliance took initiative and petitioned the EU Commission to consider the Holocaust research and archives. One important outcome is the specific mention of Holocaust research in the recitals to GDPR. Recital 158 of the 2016 final draft regulation states:

> "Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes."

More importantly, the final language of what is now Article 89 is significantly more amenable to archival and historical work. Instead of a *prima facie* prohibition, it subjects processing to the regular "appropriate safeguards":

[152] Declaration of the Stockholm International Forum on the Holocaust.

> "Article 89(1): Processing for archiving purposes… or historical research purposes… shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."

The last sentence of 89(1) still states that where the purposes of the archiving may be met with anonymized or pseudonymized data, then that must be undertaken. The continuation of Section 89 deals with caveats to other data protection rights in the case of historical research (89(2)) and archival work (89(3)). Both allow derogation from the Article 15 Right of Access by Data Subject; from the Article 16 Right to Rectification; from the Article 18 Right to Restriction of Processing; and the Article 21 Right to Object. They deviate on the Article 19 Notification Obligation regarding Rectification or Erasure of Personal Data or Restriction of Processing; and on the Article 20 Right to Data Portability; meaning, archives are able to derogate from data portability rights and from notification of the right to object.

Missing from article 89 is the right to derogate from Article 17 – the Right to Erasure, also and more memorably known as the "Right to be Forgotten" (RTBF), to which we now turn. Again, in the present context we may quote from Elie Wiesel's Nobel Lecture to briefly underscore the value of forgetting even, and especially, in the Holocaust context:

> "…it is surely human to forget, even to want to forget. The Ancients saw it as a divine gift. Indeed if memory helps us to survive, forgetting allows us to go on living. How could we go on with our daily lives, if we remained constantly aware of the dangers and ghosts surrounding us?"

RTBF was recognized by the Court of Justice of the European Union in the *Google Spain* case.[153] That case concerned a man whose financial failures from 16 years prior were showing up in Google searches, and this was presumably making it hard for him to do business now. The court found that fundamental rights under the European Charter of Human Rights were in fact engaged; this includes "Article 7 of the Charter which guarantees the right to respect for private life, whilst Article 8 of the Charter expressly proclaims the right to the protection of personal data" (para. 69). The court eventually concluded (paras. 98–99) that

[153] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* C-131/12.

> "As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public… those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name."

In other words, Gonzalez' fundamental rights override Google's interest in making all the world's data available, and the public interest in that data being available. The court qualified this:

> "However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question."

In other words, the court said that RTBF may be overridden where there is a strong interest in the general public continuing to have such access, giving an example of "the role played by the data subject in public life". So, a public figure may continue to be scrutinized many years on. That case provided ample opportunity for a full balancing of RTBF against other fundamental rights, but it was "nakedly privacy-favoring"[154] and formed the basis for RTBF in GDPR. A full consideration of RTBF and *Google Spain* is beyond the rubric of this article, but suffice for our purposes to say that, when considering RTBF in the context of Holocaust archiving, the court and subsequently GDPR have given RTBF a significant head start over conflicting rights:

> "The ECJ's categorical ruling diverges from the European Court of Human Rights on freedom of expression in conflict with privacy. Privacy was now given a presumptively preferred position in a judicial balancing when the ECJ indicated unambiguously: When in doubt, give the benefit of the doubt to informational privacy, not freedom of speech and the press."[155]

Freedom of Speech has a much richer legal and judicial legacy that the rights reflected in Holocaust archiving, and even Freedom of Speech took back seat to data protection in the *Google Spain* case. In considering Holocaust archiving, we may look to Germany's Federal Constitutional Court which has long since asserted the value that German law assigns to protecting the dignity of Holocaust victims

[154] Youm and Park, "The 'Right to Be Forgotten'", p. 282.
[155] *Ibid*., p. 283.

and their descendants, specifically through prohibition of Holocaust denial, as discussed above. In a clash of the Right to be Forgotten v the Duty to Remember, we see a clash of the human dignity of a data subject in a very concrete way, with the human dignity of millions in a nebulous form, and yet GDPR follows the court in appearing to grant *prima facie* supremacy to data protection rights. Fortunately, GDPR itself carves out exceptions to RTBF, and these reflect the limitations on RTBF, though the thresholds are set high, and it is to these we now turn to explore in specific detail how and when the Duty to Remember will overcome RTBF.

Archival and historical research considerations are expressly excluded in Article 17 itself, specifically 17(3)(d): "In so far as the right referred to… is likely to render impossible or seriously impair the achievement of the objectives of that processing." This means that, if RTBF could seriously impair the achievement of the objectives of the processing – of the archiving for our purposes, then there will be no RTBF.

Additionally, Article 17(1)(c) sets out grounds for the applicability of RTBF; briefly, if someone objects to having data about them processed, then, unless there are "overriding legitimate grounds", they have established the right of erasure. Summarizing these provisions, the following emerges: historical archives including personal data may be managed, but will need to comply with organizational measures ensuring "data minimization"; archive data ought to be adequately protected, as by pseudonymization, to the extent that such protection does not undermine the purpose of the archives; and RTBF will not apply if its application impairs the function of the archives.

This leads to the question: what are the purposes of the archives, and do pseudonymization and RTBF undermine those purposes? Since today many Holocaust institutions are especially focused on placing Holocaust materials online, we will consider the status whether that could then give rise to RTBF, and whether such processing could somehow be exempted from RTBF.

Most Holocaust archives and collections are not, or not yet, clearly defined, structured and indexed data. In many cases there is no clear picture as to what is included in the collection and the archive. In almost all cases, however, "personal data" of EU residents is involved.[156] "Personal data" is defined in GDPR Article 2 as "any information relating to an identified or identifiable natural person ('data subject')." If an archive includes names, ID numbers, etc., that will be "personal data" within the meaning of GDPR. Similarly, GDPR places even stricter limits with regard to more sensitive data, and Article 9 prohibits processing sensitive personal data, such as racial or ethnic data, data relating to political, religious or

[156] For the present discussion it is assumed that the data subjects are alive – far from obvious both because the vast majority were killed, and because survivors are now very old. Likewise, it is assumed that the data in question can be connected with an identifiable individual, and one that is protected by EU law.

philosophical beliefs, genetic and biometric data, sex and sex life, and more. There are various exceptions to this prohibition, including where it is "necessary for archiving purposes in the public interest, scientific or historical research purposes." Thus it is likely that archives have sensitive personal data, and will rely on this necessity derogation from this prohibition.

Having established, for present purposes, that we have personal data, we can quickly establish that managing an archive and putting it online will ordinarily be processing. "Processing" is defined in GDPR (Article 4.2) as: "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction", plainly then managing an archive is processing, long before material is ever put online. GDPR specifically anticipated historical research (recital 160) and archiving (recital 158) and included them within the data protection requirements. In other words, GDPR plainly applies to processing of data for archiving and for research. We will assume that Holocaust archives relate to people living in the EU, and that Holocaust archives will therefore be "processing personal data", and will be caught by GDPR.[157]

Based on these assumptions, are there grounds for an RTBF claim in the case of a Holocaust archive? To answer this, we must examine the various grounds of RTBF. RTBF does not apply automatically in every instance of data processing; there must be grounds for RTBF, and GDPR Article 17 stipulates six alternatives, each discussed briefly here.

> **17.1(a)** the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

This exception will likely not be applicable for Holocaust archives, whose purpose is generally remembrance. Some archives with a specific purpose may conceivably be caught here, but generally what such a purpose could be – restitution, tracing, etc., will apply to the heirs or family of original data subjects, such that the purpose is ongoing.

> **17.1(b)** the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

Article 6(1) stipulates that consent may form a basis for data processing, and Article 9(2)(a) does the same with respect to special categories of data. Some archives do indeed process data based on consent. These are generally victims'

[157] These are assumptions just for the present purposes. It is far from clear that Holocaust archives, given their various forms, are necessarily governed by GDPR, and there are grounds to assume that archives relate to deceased people, until demonstrated otherwise.

testimonies in writing or on video, which generally came with implied or express consent to process the data and publish it. On this basis, if someone who provided such data withdrew their consent, this would give rise to RTBF. Moreover, it is improbable that the consent given in the past will meet the stringent requirements of GDPR in this regard, suggesting that the archiving itself could be problematic if consent and its withdrawal were the basis for RTBF.

> **17.1(c)** the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

This basis is rather convoluted: Article 21(1) is the right to object to processing based on Article 6(1)(e) or (f). These are two of the six grounds in Article 6 that permit processing of personal data. The first of the two is that the data controller (in this case the archive) must engage in processing to fulfil a public interest or official function. These bases for processing – public interest or official function – will apply to many Holocaust archives. If this is the only basis on which they operate, then this section could apply. The second of the two is where the data is processed for a "legitimate interest" of the data controller (an archive) or a third party (perhaps a government institution, a claim commission, a university, survivors, etc.), with certain further exceptions. The definition of "legitimate interest" is important, but not for our analysis; let us assume for now that the archive has a legitimate interest, and that is the basis of its data processing: this would then give an opportunity for RTBF.

> **17.1(d)** the personal data have been unlawfully processed;

This is potentially a very troubling provision for Holocaust archives, particularly because the definition of "processing" is so very wide. There is no definition of "unlawful", nor any caveat as to good faith, materiality or harm. Taking an extreme position, one could argue that any processing which was not necessary is unlawful, and in an archive that has been running for any length of time there will invariably be transient, occasional, unintentional, and other such processing activities, and these could theoretically give rise to RTBF. Clearly, a counterargument would be that good-faith processing, and immaterial violations, for example, ought not to give rise to RTBF, nor perhaps to other remedies. Indeed, GDPR Article 83.2 allows for consideration of the severity of the damage to factor into the amount of the administrative fine that may be imposed:

> "regard shall be given to the… nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them."

These considerations factor into the fine, not into the RTBF. So in principle, depending on the nature of the archive and in particular on the legal basis for its processing of personal data, RTBF may apply, though liability for non-compliance may be minimal.

Having established that RTBF may in fact apply, we come to the third part of the question: is a Holocaust archive somehow exempted from the right to be forgotten? Article 17.3 sets out five bases for exemption from RTBF, each relating to whether the processing is necessary for one reason or another. Three are of particular relevance here:

**17.3(a)** for exercising the right of freedom of expression and information;

Clearly a full discussion of "freedom of expression and information", and particularly as protected in the European Convention on Human Rights, is beyond the scope of this article, but we must consider the applicability of this term to Holocaust archiving and research: would these count as "freedom of expression and information"? Some inspiration may be drawn from *Google Spain*, and Google's reaction to it. In the ruling, the court didn't provide much by way of guidance on exceptions to RTBF, though the court did note one particular example of an exception to RTBF:

> "As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question." (paras. 98-99)

For the present purposes, we may take the court's test as a proxy for the Article 17.3 right of freedom of information. Is there a preponderant interest of the general public in having access to the information in question? In order to clarify this and other crucial questions that determine the scope of Google's obligations under *Google Spain*, Google appointed an advisory council, which held several public hearings and issued a final report. At one hearing, in Paris on September 25, 2014, one of the experts invited to present to the council was an experienced information lawyer, Benoît Louvet, lawyer also for the International League against Racism and Antisemitism (LICRA). One of the points he emphasized was that RTBF must not be used to smokescreen Holocaust culpability:

> "LICRA thinks that the internet plays an essential role in transmitting the memory for the future generations here. So you have crimes against humanity from World War II. And unfortunately, there are some that are more recent ones.
> And the internet is fundamental here. It plays a fundamental role. The LICRA is worried about instrumentalization ['application' or 'manipulation' – A.S.] on the right to be forgotten by the negationists ['deniers' – A.S.]. And it is, for certain people, very tempting, people who would like to deny or to not face their responsibilities, to ask for a right to be forgotten, because they themselves are being accused of having perpetrated crimes against humanity. This is the reason why LICRA is asking for search engines, especially Google, to deal with these requests with the utmost care regarding people, individuals who might have perpetrated crimes against humanity, because memory has to be here. And it is also said that LICRA would like to say that the crimes against humanity has no prescription for our children for future generations on the internet."[158]

Google took this position very seriously, and in its brief final report specifically included Louvet's position, stipulating that "Information regarding human rights violations and crimes against humanity should weigh against delisting [i.e. against RTBF – A.S.]."[159] Notwithstanding Google's obvious and stated interest in preserving information rights to the greatest extent possible, this is an important precedent for others to follow: Google, perhaps the greatest of all data processors, has taken the position that Holocaust crime and crimes against humanity will weigh against delisting. This position predates GDPR, but is taken with respect to RTBF, which itself predates GDPR and is enshrined in it.

> **17.3 (b)** for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

This section could be especially relevant where archives are state owned and managed pursuant to law. For example, the Yad Vashem Law and the 1980 act of the US Congress establishing USHMM[160] govern Yad Vashem and USHMM respectively, but are not Union or Member State law. Poland's Museum of the History of Polish Jews, for example, is governed by a legislative instrument, an

---

[158] Available in video here, at 1:17: https://www.google.com/advisorycouncil/.
[159] "The Advisory Council to Google on the Right to be Forgotten", February 25, 2015, pp. 11-12, *ibid*.
[160] https://www.ushmm.org/m/pdfs/20100816-orig-council-charter.pdf.

order of the Minister of Culture and National Heritage from May 30, 2017, which could then form a basis for rejecting RTBF appeals.

> **17.3 (d)** for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

This section is particularly important for Holocaust archives, as they will generally be within the meaning of Article 89 archiving, as above. If RTBF is "likely to render impossible or seriously impair the achievement of the objectives" of the archive's processing, then RTBF may not apply. There are several elements here that deserve more detailed consideration and which can help construct a robust approach to Holocaust archiving in a GDPR world.

First, this section refers to "the right referred to in paragraph 1", and it is the only subsection of Article 17.3 to do so. This could be read as meaning "this specific case of RTBF", but the reference to "the right… in paragraph 1" seems to mean "RTBF generally." The difference is immense. Let us imagine an archive, and a Nazi named Ilse who asserts an RTBF claim against the archive. On the first reading, the archive must ask: "will 'forgetting' Ilse from the archives be likely to seriously impair the purpose of the archive?" Setting aside definitions of "likely, seriously, impair", etc., the answer is generally going to be "no". In most cases, an archive or collection could continue to function and serve its purpose with a name removed. On the second reading, the archive must ask: "could RTBF be likely to seriously impair the purpose of the archive?" This is rather a Kantian categorical imperative: if all people asserted RTBF, would that impair the archive? Anecdotally, my impression is that almost every Holocaust archive would likely be impaired by such RTBF assertions, and as a consequence this Article 17.3(e) ought to serve as a basis for rejection of RTBF claims.[161]

In the United States, this very question of publication and protection of data in human rights abuses was at the heart of an important case heard at the Court of Appeals of the United States. For all the differences between US and EU law and culture, this case ought to be instructive in contending with the conflicting values presented by the Right to be Forgotten v. the Duty to Remember. The American government was faced with the spectre of its own human rights abuses

[161] As indicated above, each of the terms in this section warrants further thought: likely, impair seriously, objectives. Full treatment of these will have to be left for another opportunity, but for now I will note the definition of "Processing" quoted above, which includes (Article 4) "any operation or set of operations which is performed on personal data or on sets of personal data…". The definition of "set of data" may conceivably mean an entire collection or perhaps a whole archive. It could also be construed narrowly, in which case it is more likely to impair the objective of the achievements of the objectives of that processing.

in detention facilities in Iraq, most famously Abu Ghraib – very different from the Holocaust, of course, but the comparison was made by the Second Circuit Court of Appeals. In *American Civil Liberties Union v. Department of Defense*[162] at the United States Court of Appeals, Second Circuit, the United States Department of Defense and Department of the Army ("DoD") appealed an order that they disclose 21 photographs of abuses of prisoners in Iraq and Afghanistan. The DoD claimed, in the court's summarizing words, that the "disclosure will result in unwarranted invasions of the personal privacy of the detainees they depict", justifying non-disclosure under the Freedom of Information Act 5 U.S.C. § 552 (2006). Specifically, sections § 552(b)(6) and (7)(C) were claimed to justify non-disclosure.[163] The court disagreed, and is worth citing at some length:

> "Even though we are not compelled to balance interests where there is no more than a *de minimis* privacy interest at stake, we note that contrary to the defendants' suggestion there is a significant public interest in the disclosure of these photographs. The defendants concede that these photographs yield evidence of governmental wrongdoing, but nonetheless argue that they add little additional value to the written summaries of the depicted events, which have already been made public. This contention disregards FOIA's central purpose of furthering governmental accountability, and the special importance the law accords to information revealing official misconduct… Governmental misconduct is conceded here… and we accordingly note that the public interest in disclosure of these photographs is strong. In any event, there is no more than a *de minimis* privacy interest in withholding the redacted photographs."[164]

That case concerned government misconduct, and FOIA in all jurisdictions is intended as a form of check on government abuse of power. Holocaust archives rarely relate, these days, to government power. But they serve the same function in checking abuse of power by governments, by revealing misconduct, increasing accountability, and thereby demotivating abuses. The position of that court is, basically, the bold answer to all claims of privacy against revelations of Holocaust crimes, misappropriated assets or even undisclosed assets: the revelation of such information is crucial to justice and to property rights. The invasions of privacy are generally *de minimis* in and of themselves, and are dwarfed by the purpose served.

---

[162] 543 F.3d 59 (2008).

[163] "This section does not apply to matters that are… – personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; – records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information… could reasonably be expected to constitute an unwarranted invasion of personal privacy."

[164] *Ibid*., pp. 87-88 , footnotes omitted.

In addition, the paternalistic claim of privacy violation on behalf of a victim who has not made that claim himself/herself ought to be a red flag suggesting that privacy is being used as a smoke screen.

The court, responding to DoD's claim that dissemination of the images would violate the Geneva Convention, made the following observation, particularly pertinent to our subject matter:

> "At the end of the [Second World] war, the United States government widely disseminated photographs of prisoners in Japanese and German prison and concentration camps… These photographs of emaciated prisoners, corpses, and remains of prisoners depicted detainees in states of powerlessness and subjugation similar to those endured by the detainees depicted in the photographs at issue here. Yet the United States championed the use and dissemination of such photographs to hold perpetrators accountable."[165]

The court noted that the US government itself had disseminated photographs of concentration camp prisoners, and used them as a tool for accountability. Clearly the situation in the US is very different from Europe, and in most cases Holocaust research is not applied for government accountability purposes. But as follows form the court's comparison, the principles of accountability are the same whether applied to a sitting government, or to nonagenarians, or to banks or insurance companies, to industry and even to revisionist historians or Holocaust deniers. For all the details of data protection law, some creative and bold solutions will occasionally be necessary to do justice. Frederick Ketelaar, an archivist and theoretician of archiving, noted a few years back as follows:

> "Many of the files created during and after World War II that are now being used in the processes of restitution and compensation for Holocaust assets should have been destroyed, according to the criteria of both the European Data Protection directive and most professionally accepted criteria for archive appraisal. One of the lessons learned is that files created under unprecedented circumstances in an extraordinary era – for example, during or after war, revolution, natural or man-made disasters, or political or economic crises – have to be appraised differently from those created in the course of 'normal' human business."[166]

Creative legal work may be required to ensure that data protection does not stifle Holocaust archiving and research,[167] and GDPR Recital 158 allows for

---

[165] N.163, p. 89.

[166] Ketelaar, *The Panoptical Archive*, p. 145.

[167] Perhaps an international pool of data protection risk, or a more traditional insurance model, would enable Holocaust research institutions to take a bold position with respect to data protection.

member state legislation in this field, which now ought to be used to clarify and improve the legal status of Holocaust archives vis-à-vis data protection. German media theorist Wolfgang Ernst has asserted that "[a]rchival memory became… an instrument in the National Socialist programme for annihilation of European Jewry"[168] – meaning that the archives and records were used by Nazis to kill as quickly and efficiently as possible. Holocaust researchers and archivists and EU legislators have a responsibility to ensure that the same is true in the reverse: archival memory is crucial to restitution, education and the continued revival of survivors' identities, and Holocaust archives must not be allowed to lapse into misuse on account of data protection principles.

In summary, we have seen that many significant data protection legal issues arise for Holocaust archives and online access, and that more generally there is a significant clash of values in the meeting of the Duty to Remember and the Right to be Forgotten. However, in many cases there are partial or more complete solutions to the legal challenges that Holocaust archives face. In some cases, open questions remain to be answered on a case-by-case basis, and in some cases bold positions ought to be taken to ensure that data protection does not cow Holocaust history into submission. Member state legislation may be required, Data Protection Authorities, WP29 and other state and EU institutions may be a part of the solution, and archives themselves may be bold and take legal positions that set important precedent in ensuring that data protection does not get in the way of Holocaust archiving, that the Right to be Forgotten does not overtake the Duty to Remember.

## Conclusion

Modern European privacy and data protection laws arose largely in reaction to the horrors of authoritarian rule generally, and the Holocaust specifically. Ironically, and sadly, privacy has been a consistent barrier to Holocaust justice, and rather than serve the dignity of the victims of the Holocaust, it has done the opposite: it perpetuated the dehumanizing crimes they suffered, denying them a voice, justice and restitution. Several specific examples have been discussed here, including: the Data Theory of the Dutch Holocaust – one of the prevalent justifications for European Data Protection law – has long masked the extensive collaboration of Dutch state institutions with the Holocaust; the International Tracing Service refused to share its archives with Holocaust victims groups and research institutions on account of privacy considerations; privacy prevented important Holocaust justice and research from being publicized, used and disseminated; and privacy prevented banks, insurance companies and others from

[168] Ernst, "Archival Action", in *History of the Human Sciences* 12, 1999, pp. 13-34, 25; quoted in Ketelaar, "Archival Temples", p. 226.

making adequate restitution, or indeed – for decades at least – any restitution. There have been few approaches that have assigned significant value to Holocaust research and considered data protection rights in light of that value; of particular note are the opinion of the Hungarian DPA, Google's approach as indicated in the final report of its Advisory Council on RTBF, the Second Circuit Court of Appeals in the *ACLU* case, and the position advocated by USHMM with regard to ITS.

The Holocaust informs other mass human rights violations and their legal treatment, and conclusions drawn with respect to Holocaust justice have rightly been instrumental in the process of justice following other atrocities. One important general conclusion from this paper is that the claim and use of privacy in severe human rights violation cases ought to be a bright red flag, as human rights and human dignity aspects of justice and restitution must not be blocked by privacy of the victim, especially where the victim has not claimed otherwise, and must not be obstructed by the privacy of the perpetrators. A second conclusion is that data protection considerations must not be a smokescreen for atrocities, nor for the research and education that must follow from those atrocities, even generations later. The law increasingly recognizes such tools as Non-Disclosure Agreements, anonymization and pseudonymization, and Privacy-Shield-like arrangements, which can all be applied, though these are often poor substitutes for publication of facts, documents, processes and names. Indemnification, insurance and other forms of reducing and sharing risk can also enable freer publication. The interests of justice and memorialisation generally, and the dignity and the rights of the victims specifically, are almost always better served by publicity.

Archives and researchers have several avenues to taking an approach on the permissive side of data use for Holocaust research. It is hoped that they will make use of these, and support each other in such an approach. At the legislative levels, as enabled by GDPR, EU member states may legislate to facilitate Holocaust research, and at the regulatory level, DPAs may follow the lead of the Hungarian DPA in showing a sophisticated value-based appreciation for Holocaust research and archiving.

# REFERENCES


- Aalders, Gerard, *Nazi Looting: The Plunder of Dutch Jewry during the Second World War*, New York, Berg, 2004.
- Allen, Anita, *Unpopular Privacy*, Oxford, OUP, 2011.
- Bazyler, Michael J., *Holocaust Justice: The Battle for Restitution in America's Courts*, New York, NYU, 2005.
- Belkin, P., "CRS Report: Opening of the International Tracing Service's Holocaust-Era Archives in Bad Arolsen, Germany", 2007.
- Ben-Naftali, O. and Y. Tuval, "Punishing International Crimes Committed by the Persecuted: The Kapo Trials in Israel (1950s-1960s)", in *Journal of International Criminal Justice* 4, 2006, 128.
- Bennett, Colin J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell, 1992.
- Bennett Colin J. and Charles D. Raab, *The Governance of Privacy – Policy Instruments in Global Perspective*, Cambridge, MIT Press, 2006.
- Bennett, G. H., "The Limits of West German Justice in the 1960s: The Post-War Investigation of Walter Gieseke", in *Law, Crime and History* 2, 2013, 116-139.
- Bergier, Jean-François *et al.*, "Final Report of the Independent Commission of Experts Switzerland – Second World War", 2002.
- Biedermann, C., "50th Anniversary of the ITS: International Tracing Service: 50 years of service to humanity", in *International Review of the Red Cross* 33, 1993, 447-456.
- Bignami, F., "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining", in *Boston College Law Review* 48, 2007, 609.
- Black, Edwin, *IBM and the Holocaust*, New York, Crown, 2001.
- Bloch-Wehba, H., "Confronting Totalitarianism at Home: The Roots of European Privacy Protections", in *Brooklyn Journal of International Law* 40, 2015, 749.
- Bloustein, E., "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", in *New York UL Rev* 39, 1964, 962.
- Browning, Christopher R., *Ordinary Men: Reserve Police Battalion 101 and the Final Solution in Poland*, London, Harper Collins, 1993.
- Brunelle, K., "A Brief Historical Evolution of the International Tracing Service (ITS): The Largest Collection of Holocaust Related Documents", in *School of Library and Information Science Journal* 3:2, 2014.
- Bryant, Michael S., *Eyewitness to Genocide: The Operation Reinhard Death Camp Trials, 1955–1966*, Knoxville, University of Tennessee Press, 2014.

- Burkert, H., "Privacy – Data Protection: a German / European Perspective", in *Proceedings of the Second Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council*, 1999.
- Byrne, G., "Legal Theory and The Holocaust: Between The Purposive and The Reflective", in *The Journal Jurisprudence,* 2013, 373-397.
- Cassese, Antonio (ed.), *The Oxford Companion to International Criminal Justice*, Oxford, OUP, 2009.
- Cohen, Boaz, *Israeli Holocaust Research: Birth and Evolution*, New York, Routledge, 2013.
- Cook, Terry, *Remembering the Future: Appraisal of Records and the Role of Archives in Constructing Social Memory*, in Francis X. Blouin and William G. Rosenberg (eds.), *Archives, Documentation, and Institutions of Social Memory: Essays from the Sawyer Seminar*, Michigan, UMich, 2007.
- Cooper, John, *Raphael Lemkin and the Struggle for the Genocide Convention*, London, Palgrave, 2008.
- Croes, Marnix, "The Holocaust in the Netherlands and the Rate of Jewish Survival", in *Holocaust Genocide Studies* 20:3, 2006, 474-499.
- Douglas, L., "Wartime Lies: Securing the Holocaust in Law and Literature", in *Yale Journal of Law and the Humanities* 7, 1995.
- Dreyfus, J., "Opening the Nazi archives at Bad Arolsen", in *Books and Ideas* 6, 2013.
- Eberle, E.J., "Human Dignity, Privacy, and Personality in German and American Constitutional Law", in *Utah Law Review*, 1997, 963.
- Eizenstat, Stuart E., *Imperfect Justice: Looted Assets, Slave Labor, and the Unfinished Business of World War II*, New York, Public Affairs, 2009.
- Ernst, Wolfgang, "Archival Action: The Archives as ROM and its Political Instrumentalization under National Socialism", in *History of the Human Sciences* 12, 1999, 13-34.
- Ernst, Wolfgang, *Digital Memory and the Archive*, Minnesota, University of Minnesota Press, 2013.
- Findlay, Mark J., *International and Comparative Criminal Justice: A Critical Introduction*, Oxford, Routledge, 2013.
- Flaherty, David H., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*, Chapel Hill, North Carolina Press, 1989.
- Fraser, David, *Law After Auschwitz: Towards a Jurisprudence of the Holocaust*, Durham, NC, Carolina Academic Press, 2005.
- Gerstenfeld, M., "Jewish War Claims in the Netherlands", in *Jewish Political Studies Review* 12, 2000.
- Gerstenfeld, M., *Judging the Netherlands: The Renewed Holocaust Restitution Process 1997-2000*, Jerusalem, Jerusalem Center for Public Affairs, 2011.

- Gilreath, S., "The Internet and Inequality: A Comment on the NSA Spying Scandal", in *Wake Forest L. Rev*. 49, 2014, 525.
- González Fuster, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Switzerland, Springer, 2014.
- Höss, Rudolph, *Commandant of Auschwitz*, London, Phoenix Press, 2000.
- Ketelaar, E., "Archival Temples, Archival Prisons: Modes of Power and Protection", in *Archival Science* 2*,* 2002, 221-238.
- Ketelaar, E., *The Panoptical Archive*, in Francis X. Blouin and William G. Rosenberg (eds.), *Archives, Documentation, and Institutions of Social Memory. Essays from the Sawyer Seminar*, Ann Arbor, University of Michigan Press, 2006, 144-150.
- Kosta, Eleni, *Consent in European Data Protection Law*, Leiden, Brill, 2013.
- Krotoszynski Jr., R., "The Polysemy of Privacy", in *Indiana Law Journal* 88, 2013, 908.
- Lasik, Aleksander, *Historical-Sociological Profile of the Auschwitz SS*, in Yisrael Gutman and Michael Berenbaum (eds.), *Anatomy of the Auschwitz Death Camp*, Indiana, Indiana University Press, 1998.
- Lasik, Aleksander, *Postwar Prosecution of the Auschwitz SS*, in Yisrael Gutman and Michael Berenbaum (eds.), *Anatomy of the Auschwitz Death Camp*, Indiana, Indiana University Press, 1998.
- Lazer, D. and V. Mayer-Schonberger, "Statutory Frameworks for Regulating Information Flows: Drawing Lessons for the DNA Data Banks from other Government Data Systems", in *Journal of Law, Medicine and Ethics* 34:2, 2006, 366.
- Less, S., "International Administration of Holocaust Compensation: The International Commission on Holocaust Era Insurance Claims (ICHEIC)", in *German Law Journal* 9:11, 2008, 1651.
- Levin, Itamar, *Kapo in Tel Aviv: Prosecution in Israel of Jews Accused of Collaboration with the Nazis*, Jerusalem, Moreshet, 2015.
- Lichtblau, Eric, *The Nazis Next Door: How America Became a Safe Haven for Hitler's Men*, Boston, Mariner, 2014.
- Lindeman, Y. and H. de Vries, *Resistance and Rescue in the Netherlands*, in Patrick Henry (ed.), *Jewish Resistance Against the Nazis*, Washington, DC, Catholic University of America Press, 2014.
- Lippman, M., "Genocide: The Trial of Adolf Eichmann and the Quest for Global Justice", in *Buffalo Human Rights Law Review* 8, 2002, 45.
- Lloyd, Ian J., *Information Technology Law*, Oxford, OUP, 2014.
- McDonald, C., "Reconciling Holocaust Scholarship and Personal Data Protection: Facilitating Access to the International Tracing Service Archive", in *Fordham International Law Journal* 30:4, 2006, 1360-1391.
- McKale, Donald M., *Nazis After Hitler*, Maryland, Rowman, 2012.
- Mills, Jon L., *Privacy: The Lost Right*, Oxford, OUP, 2008.
- Moore, Robert, *Victims and Survivors: The Nazi Persecution of the Jews in the Netherlands, 1940-1945*, London, Arnold, 1997.

- Naftali, Timothy, *The CIA and Eichmann's Associates*, in Richard Breitman *et al.* (eds.), *U.S. Intelligence and the Nazis*, Washington, DC, National Archives Trust Fund Board, 2005.
- Neuborne, B., "Preliminary Reflections on Aspects of Holocaust-Era Litigation in American Courts", in *Washington University Law Quarterly* 80, 2002, 795.
- Ohm, P., "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", in *UCLA Law Review* 57, 2009, 1701.
- Pech, Laurent, *The Law of Holocaust Denial in Europe: Towards a (Qualified) EU-Wide Criminal Prohibition*, in Ludovic Hennebel and Thomas Hochmann (eds.), *Genocide Denials and the Law*, New York, OUP, 2011.
- Pendas, D., "'I didn't know what Auschwitz was': The Frankfurt Auschwitz Trial and the German Press, 1963-1965", in *Yale Journal of Law and Humanities* 12, 2000, 397.
- Pendas, David O., *The Frankfurt Auschwitz Trial, 1963-1965*, Cambridge, Cambridge University Press, 2006.
- Pérez, Maria V. and Pablo Palazi, *Défis du droit de la protection de la vie privée – Perspectives du droit européen et nord-américain*, Cahiers du Centre de Recherche Informatique et Droit 31, 2008, 245.
- Pinchevski, A., T. Liebes and O. Herman, "Eichmann on the Air: Radio and the Making of an Historic Trial", in *Historical Journal of Film, Radio and Television* 27:1, 2007, 1-25.
- Presser, Jacob, *Ashes in the Wind: The Destruction of Dutch Jewry*, Detroit, Wayne State University Press, 1988.
- Reidenberg, J. R., "Resolving Conflicting International Data Privacy Rules in Cyberspace", in *Stan. Law Rev*. 52, 2000, 1315.
- Riccardi, J. Lee, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?", in *Boston College of International and Comparative Review* 6, 1983, 243.
- Richie, George E., "The Role of the Epistemic Community in Influencing Privacy Legislation: The United States and the European Union", Dissertation, Denver, 2010.
- Schreiber, A., "Privacy: Proprietary or Human Right? An Israeli Law Perspective", in *Intellectual Property Quarterly* 1, 2009, 99.
- Seltzer, William and Margo Anderson, *Using Population Data Systems to Target Vulnerable Population Subgroups and Individuals: Issues and Incidents*, in Jana Asher, David Banks and Fritz J. Scheuren (eds.), *Statistical Methods for Human Rights*, New York, Springer-Verlag, 2007, 273-328.
- Singer, I. M., "Reductio Ad Absurdum: The Kapo Trial Judgments", in *International Criminal Law Jurisprudence and Customary International Law* 24(2), 2013, 235-258.
- Shapiro, P., "History Held Hostage", in *Reform Judaism*, 2009, 42.
- Shapiro, P., Foreword to S. Brown-Fleming, *Nazi Persecution and Post-War Repercussions*, Lanham, Rowman & Littlefield, 2016.
- Solove, Daniel, *Understanding Privacy*, Cambridge, HUP, 2008.
- Spiekermann, S., *Ethical IT Innovation: A Value-Based System Design Approach*, Boca Raton, Taylor and Francis, 2015.

- Stern, J., "Judgment in the Shadow of the Holocaust: Section 2: New Perspectives on the Eichmann Trial: The Eichmann Trial and Its Influence on Psychiatry and Psychology", in *Theoretical Inquiries into the Law* 1, 2000, 393.
- Viola de Azevedo Cunha, Mario, *Market Integration Through Data Protection: An Analysis of the Insurance and Financial Industries in the EU*, Dordrecht, Springer, 2013.
- Vrdoljak, A. F., "Human Rights and Genocide: The Work of Lauterpacht and Lemkin in Modern International Law", in *EJIL* 20:4, 2009, 1163-1194.
- Waltzer, K., "Opening the Red Cross International Tracing Service Archive", in *J. Marshall J. Computer and Info. L.* 26, 2009, 161.
- Warren, S. and L. Brandeis, "The Right to Privacy", in *Harvard Law Review* 4, 1890, 193.
- Winn, Jane K., *Can a duty of information security become special protection for sensitive data under US Law?*, in Paul Weindling (ed.), *Victims and Survivors of Nazi Human Experiments*, London, Bloomsbury, 2014.
- Wittmann, J., "The Two Western Cultures of Privacy: Dignity versus Liberty", in *Yale L.J.* 113, 2004, 1151-1221.
- Wittmann, Rebecca, *Beyond Justice: The Auschwitz Trial*, Cambridge, Harvard University Press, 2005.
- Wolf, Diane L., *Beyond Anne Frank: Hidden Children and Post-War Families in Holland*, Berkeley, University of California, 2007.
- Yablonka, H., "Justice for Nazis and their Collaborators Law – A Further Aspect to the Question of Israelis, Survivors, and the Holocaust" (Heb), in *Katedra* 82, 1997, 135.
- Youm, K. H. and A. Park, "The 'Right to Be Forgotten' in European Union Law: Data Protection Balanced With Free Speech?", in *Journalism & Mass Communication Quarterly* 93(2), 2016, 273-295.
- Zabludoff, Sidney, *ICHEIC: Excellent Concept but Inept Implementation*, in Michael J. Bazyler and Roger P. Alford (eds.), *Holocaust Restitution: Perspectives on the Litigation and Its Legacy*, New York, NYU Press, 2006.