A GLIMPSE AT GERMAN PRIVACY LAWS, FROM A DARK PAST TO THE STRICTEST DATA PROTECTION LAWS IN EUROPE (BUT THERE IS STILL A LONG WAY TO GO)

Cody Valdez*

On May 12, 2017, WanaCrypt0r 2.0, spread across the globe in one of the largest ransomware[1] attacks ever, and likely used the National Security Agency's EternalBlue exploit released by ShadowBrokers in April 2017.[2] There have been more than 300,000 detections of WanaCrypt0r 2.0 in 150 countries.[3] The prevalence of cyber-attacks, among other concerns, has led to an increasing percentage of American's lacking confidence there personal information is private and secure.[4] Invasion of privacy is not a new concept, rather it is a concept people all around the world are far too familiar with. This paper will examine how far one such country whose government subjected its people to some of the worst invasion of privacy atrocities during the Third Reich, Germany. It will contrast the state of privacy in Nazi German and Germany's current information privacy rights laws; and ask "where do we go from here?"

I. "PRIVACY" IN NAZI GERMANY

From 1933 until 1939, more than 400 decrees and regulations that restricted all aspects of the public and private lives

---

* Associate Nuremberg Editor, Rutgers Journal of Law and Religion; Juris Doctor Candidate May 2018. Rutgers Law School.

[1] Ransomware is a form of malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data "hostage" until the victim pays a ransom, frequently by demanding payment in Bitcoin. Ben Rossen, *Ransomware – A closer look*, FEDERAL TRADE COMMISSION (Nov. 10, 2016, 11:05 AM), https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look.

[2] Chris Graham, *NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history*, THE TELEGRAPH NEWS (MAY 20, 2017, 1:36 AM), http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

[3] *Id.*

[4] Consumer Reports, *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds (May 11, 2017),* http://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/ (last visited Aug. 8, 2017).

of Jews in Germany.[6] Many laws were national and issued by the German administration and affected all Jews.[7] State and regional laws were also enacted by officials leaving no corner of Germany untouched.[8]

The most infamous Anti-Semitic Legislation was from 1933 to 1939. This included the Nuremberg Race Laws made up of the Reich Citizenship Law and the Law for the Protection of German Blood and German Honor, the latter of which excluded German Jews from Reich citizenship and prohibited them from marrying or having sexual relations with persons of "German or German-related blood."[9]

The Decree against Public Enemies (Folk Pest Law), enacted on September 5, 1939 just 4 days after the beginning of WWII when Germany invaded Poland, made it a crime against person or property, or against the community or public security could carry a death sentence if the accused was charged with exploiting the special conditions of war.[10] The Decree against Public Enemies was likely the most frequently used legal basis for the handing down of approximately 15,000 death sentences by the Courts from 1941 to 1945.[11]

A premier example of how these laws worked to strip the privacy of people is the Katzenberger case. Leo Katzenberger was a prominent Jewish businessman in Nuremberg who owned many stores throughout southern Germany, and was a very prominent figure in the Jewish community of Nuremberg.[12] Katzenberger's businesses were "Aryanized[13]" in 1938, but he was still considered

---

[6] United States Holocaust Memorial Museum, Anti-Jewish Legislation in Prewar Germany, U.S. HOLOCAUST MEMORIAL MUSEUM, https://www.ushmm.org/wlc/en/article.php?ModuleId=10005681. (last visited Aug. 8, 2017).

[7] *Id.*

[8] *Id.*

[9] The Nuremberg Laws did not identify a "Jew" as someone with particular religious beliefs. Rather, the first amendment to the Nuremberg Laws defined anyone who had three or four Jewish grandparents as Jew, regardless of whether that individual recognized himself or herself as a Jew or belonged to the Jewish religious community. *Id.*

[10] United States Holocaust Memorial Museum, *Decree Against Public Enemies (Folk Pest Law)*, https://www.ushmm.org/wlc/en/article.php?ModuleId=10007906.

[11] *Id.*

[12]United States Holocaust Memorial Museum, *Katenberger Case, March13, 1942*, ushmm.org, https://www.ushmm.org/wlc/en/article.php?ModuleId=10007908 (last visited September 17, 2017)

[13] "Aryanization" of Jewish businesses, was a process involving the dismissal of Jewish workers and managers, as well as a transfer of the companies and

well off.[14] Katzenberger continued to own his building where he rented a small apartment to Irene Steiler.[15] In 1941, Katzenberger, a 76-year-old man, was accused of having a sexual affair with Seiler, a 30-year-old woman, and arrested on charges of race defilement.[16] Both Katzenberg and Seiler repeatedly denied ever having any sexual relations.[17] However, the Court convicted Katzenberger of race defilement and sentenced Leo Katzenberger to death by beheading.[18] The Court applied the Folk Pest Law which permitted death because Mr. Katzenberger was accused of exploiting wartime conditions to further his crime on the grounds that he secretly visited Seiler "after dark."[19] This was a deliberately orchestrated show trial, in which the judge referred to Katzenberger several times as a "syphilitic Jew" and an "agent of world Jewry."[20]

In 1937 and 1938 the government enacted legislation meant to impoverish Jews and remove them from the German economy by requiring them to register their property.[21] During his speech on November 10, 1938 after the "Night of Broken Glass"[22], Julius

---

enterprises to non-Jewish Germans, who bought them at prices fixed well below market value. United States Holocaust Memorial Museum, *Anti-Jewish Legislation in Prewar Germany*, ushmm.org, *https*://www.ushmm.org/wlc/en/article.php?ModuleId=10005681(last visited September 17, 2017)

[14] *Holocaust Encyclopedia, Katzenberger Case, March 13,* 1942, UNITED STATES HOLOCAUST MEMORIAL MUSEUM, https://www.ushmm.org/wlc/en/article.php?ModuleId=10007908 (last visited May 16, 2017).

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Katzenberger, supra* note 14.

[20] *Id.*

[21] *Holocaust Encyclopedia, Anti-Jewish Legislation in Prewar Germany*, UNITED STATES HOLOCAUST MEMORIAL MUSEUM, https://www.ushmm.org/wlc/en/article.php?ModuleId=10005681 (last visited May 19, 2017).

[22] On November 9, 1938, Ernst vom Rath a German diplomat in Paris, died from his wounds after being shot two days prior by a seventeen-year-old Jew whose family was the victim of Nazi anti-Semitic policies. Lead by Joseph Goebbels, at Hitler's approval, the Nazi's organized nationwide attacks on Jews in Germany. During the "Night of Broken Glass" (*Kristallnacht*), over 1,500 synagogues were burned down, thousands of Jewish shops were destroyed, Dozens of Jews were killed, and tens of thousands were arrested. The Nazi's said this was a "spontaneous" reaction to Vom Rath's death. Randall L. Bytwerk, Landmark Speeches of National Socialism 86 (Martin J. Medhurst, 2008).

Streicher[23] spoke to a crowd of almost 100,000 people at "Adolf Hitler Square" in the center of Nuremburg, applauding the people for their "restraint" the night before, and painting a vision of the future where they would be rewarded with riches that once belonged to the Jews when he said:

> [T]he time will come when Germans no longer live in barracks, but rather the Jews. Germans will then move into the fine houses. And if the Jews now move away, we will be able to give pleasure to some families with many children by allowing them to celebrate Christmas in a decent home, a home in which others previously celebrated a different holiday. The mayor will see to it that everything possible is done in the near future to relieve our present housing shortage. And the Führer has assured us that, especially in Nuremberg, more will be done to alleviate the tragic inheritance others left to us. The good will is there but you all know the state Germany was in, and what must be done to make us secure.[24]

This small sample displays the complete lack of privacy expectation that could be had in Germany under the reign of Hitler. To aid the Nazi's in carrying out targeted attacks against Jews, among others, the Third Reich systematically abused the private data it collected.[25] For example, the Third Reich maintained an index of Jews that listed the identity of all Jews dating back to their grandparents' generations.

II. GERMANY PUSHES INFORMATION PRIVACY AND DATA PROTECTION TO THE FUTURE

From the archaic atrocities of World War II to being at the forefront in information and data privacy today, Germany has made vast strides in the area of privacy. Germans place a great deal of

---

[23] Julius Streicher, one of Hitler's earliest followers, was the most prominent and crudest Nazi anti-Semite, and published the weekly newspaper *Der Stürmer* between 1923 and 1945. *Id.*

[24] *Id.*

[25] Alvar Freude and Trixy Freud, *Echos of History: Understanding German Data Protection*, bfna.org, http://www.bfna.org/publication/newpolitik/echos-of-history-understanding-german-data-protection (October 2016)

importance on privacy and data protection.[26] Fear of the privacy sector and, even more so, government abuse of personal data is widespread, and German law, in turn, grants its citizens a great deal of protection.[27]

Germany's constitution (the Basic Law) does not explicitly enshrine data protection, rather Germany's highest court, the Federal Constitution Court, granted the protection in what is known as the "census ruling."[28] This 1983 landmark decision, in which the court held that citizens have a basic right of self-determination with regards to their personal data, was in response to the census that became the subject of numerous constitutional complaints of violations of respondents' civil rights.[29] The decision compelled the federal government to separate personal data from the census questionnaires and ensure greater anonymity for survey-takers.[30]

World War II left a deep mark on its citizens resulting in Germans feeling strongly about data protection – specifically, protection of the citizen against abuse of his or her data – and protection of privacy.[31] Today Germany has derived many specific laws that govern how data may be handled such as: the Federal Data Protection Act, the Telecommunications Act, the Telemedia Act, as well as the Criminal and Civil Codes.[32]

The decision compelled the federal government to separate personal data from the census questionnaires and ensure greater anonymity for survey-takers.[33]

World War II left a deep mark on its citizens resulting in Germans feeling strongly about data protection – specifically, protection of the citizen against abuse of his or her data – and protection of privacy.[34] Today Germany has derived many specific laws that govern how data may be handled such as: the Federal Data Protection Act, the Telecommunications Act, the Telemedia Act, as well as the Criminal and Civil Codes.[35] Germany's Federal Data Protection Act is a comprehensive body of law, this is unlike the United States, which has sector specific laws (e.g. Health

---

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Freude*, *supra* note 25.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*

Insurance Portability and Accountability Act (HIPAA)[36]; Gramm-Leach-Bliley Act (GLBA)[37]; and Children's Online Privacy Protection Act (COPPA)[38]). [39]

The rest of this section will focus on Germany's Federal Data Protection Act which was amended in 2009, its purpose is to protect the individual against his or her right to privacy being impaired through the handling of his or her personal data.[40] The scope of the act applies it to the:

> [C]ollection, processing and use of personal data by:
>
> 1. public bodies of the Federation,[41]
>
> 2. Public bodies of the Länder[42] in so far as data protection is not governed by Land legislation and in so far as they:
>
> a) execute federal law or,

---

[36] HIPPA required the U.S. Department of Health and Human Services to promulgate comprehensive regulations to protect the privacy and security of personal health information. PETER P. SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS, AND PRACTICES 42 (Terry McQuay ed., 2012).

[37] The GLBA applies broadly to financial institutions (any company "significantly engaged" in financial activities in the United States), and address the handling of nonpublic personal information's, which includes a consumer's name and address, and the consumer's interactions with banks, insurers and other financial institutions. Id. at 43.

[38] COPPA applies to the operators of commercial websites and online services that are directed to children under the age of thirteen. Id.

[39] Freude, s*upra* note 25.

[40] Bundesdatenschutzgesetz [Federal Data Protection Act], Jan. 15, 2003, Federal Law Gazette I at 66, last amended by Federal Law Gazette I at 2814, art. 1, Aug. 14, 2009, https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0009.

[41] "Public bodies of the Federation" means the authorities, the bodies of the judicature and other public-law institutions of the Federation, of the Federal corporations, establishments and foundations under public law as well as of their associations irrespective of their legal structure. The successor companies created from the Special Fund Deutsche Bundepost by act of law are considered public bodies as long as they have the exclusive right under the Postal Law. *Id.*

[42] "Public Bodies of the Länder" means the authorities, the bodies of the judicature and other public-law institutions of a Land, of a municipality, an association of municipalities or other legal persons under public law subject to Land supervision as well as of their associations irrespective of their legal structure. *Id.*

> b) act as bodies of the judicature and are not dealing with administrative matters,
>
> 3. private bodies in so far as they process or use data by means of data processing systems or collect data for such systems, process or use data in or from non-automated filing systems or collect data for such systems, except where the collection, processing or use of such data is effected solely for personal or family activates.[43]

For the purposes of the act "Personal data" means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject).[44] The Act regulates any collection, use or processing of personal data.[45] The Act covers cases where: (1) the data controller is located in Germany and the processing is carried out in Germany or within the EU; (2) the data controller is located in another EU member state but the collection, processing or use of personal data is carried out by a branch in Germany; and (3) the data controller is not located in an EU member state but collects, processes or uses personal data in Germany.[46] However, the Act does not apply if the data controller is located in another EU member state but collects, processes or uses personal data in Germany.[47]

The Act covers a broad range of data collection issues, including a requirement of notification of data security breaches and changes in data marketing rules.[48] Additionally, the amendments increased fines for violations of the law.[49]

---

[43] Die Übersetzung berücksichtigt die Änderung(en) des Gesetzes durch Artikel 1 [Federal Data Protection Act], Aug. 14, 2009, BGBL I at 2814 (Ger.), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0009

[44] *Id.*

[45] Norbert Nolte & Christoph Werkmeister, *Data protection in Germany: overview*. https://content.next.westlaw.com/3-502-4080?transitionType=Default&contextData=(sc.Default)&__lrTS=20170514211411389&firstPage=true&bhcp=1

[46] *Id.*

[47] *Id.*

[48] Laura Ybarra, Note and Comment, *The E.U. Model as an Adaptable Approach for U.S. Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany, and the United States*, 34 Loy. L.A. Int'l & Comp. L. Rev. 267, 267-268 (2011).

[49] *Id.* at 285.

German data protection laws are the strictest data collection laws in Europe.[50] In Germany, data protection often rests on complex "balance" provisions.[51] In many circumstances within the private sector, data processing for secondary purposes is allowed without consent, and the balancing test used in this context favors the private sector.[52] However, this test is also employed for the public sector, but provisions have been implemented that limit data collected specifically by the body carrying out the task.[53] When the balance test is used in these instances, the balance is "tilted against the public sector."[54]

Even with the strictest data protection laws in Europe, Germany's enforcement system is not as strong as might be expected.[55] In the public sector, the role of the federal and state data protection commissioners is limited.[56] The federal commissioner can demand a formal review but cannot order specific changes, and thus, the commissioner lacks significant legal power.[57] However, in the private sector, supervisory authorities are granted extensive enforcement and investigatory powers, and can demand "any information which the supervisory authority needs for the fulfillment of its task," and the information must be provided without delay.[58] The supervisory authority can also set a deadline for the compliance of certain measures and impose administrative fines.[59]

III. WHERE TO GO FROM HERE

This note is meant to display the continuing struggle faced with information privacy that has become more apparent today with an ever expanding Internet of Things (IoT). With more and more people around the world creating large amounts of data that is being

---

[50] *Id.* at 283.
[51] *Id.* at 284.
[52] *Id.*
[53] This is stricter than even the EU Data Protection Directive which allows for processing with it is "necessary for the performance of the task carried out in the public interest of in the exercise of official authority." Possible rephrasing "This is more strict than the EU Data Protection Directive, which allows for processing when it is "necessary for the performance of the task carried out in the public interest in the exercise of official authority.*" Id.* at 285.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*

collected on a daily basis, one should be concerned with how that data is collected; where it is going; how it is stored—and so much more.

The past of Nazi Germany shows how much can be accomplished and executed by having an "index" of Jewish people. Today, throughout the world, companies and governments have indexes storing a lot more than an individual's religious belief and ancestry. That almost seems mundane compared to the amount of data produced and collected now. With attacks such as WanaCrypt0r 2.0 ever lurking to hack companies, and steal or encrypt the personal information of everyone stored on that system the need data protection laws to protect the personal data of the citizens of each country is more important now than ever.

Germany is a prime example that even today, the strictest data protections laws in Europe, while taking leaps and bounds from World War II, are still lacking in the authority granted to commissioners and require complex balancing tests. As data protection continues in the future, it may be wise to look toward Germany as they continue shape the future. In fact, this is already happening and the new comprehensive EU General Data Protection Regulation (GDPR) goes into effect on May 25, 2018 and is designed to bring every country in the EU up to the same standards and harmonize data privacy laws across Europe.[60]

Whether or not comprehensive models, such as the GDPR are the future of data protection laws remains to be seen, however, one thing is clear for the future, collaboration, communication, and information sharing between nations, governments, and the public and private sectors that was a necessity in formulating the GDPR will continue to be a necessity to combat the wide array of attacks and prevent attacks in the future. For now, one can only hope that collaboration between all sectors will only grow and become more transparent in an effort to protect each country's constantly expanding infrastructure.

In conclusion, it is important to note that all the laws and regulations on companies storing the information of citizens in their respective countries can only do so much. It is up to each person practice good cyber hygiene, protect, and monitor their information as well. WanaCrypt0r 2.0 would not have taken the world by storm

---

[60] *GDPR Portal: Site Overview,* THE EU GENERAL DATA PROTECTION REGULATION, http://www.eugdpr.org (last visited May 19, 2017).

on May 12, 2017 if the infected computers had been updated with the Microsoft patch update, released in March 2017.[61]

[61] Kevin Murnane, *How To Protect Yourself From The Global WanaCry Ransomware Attack*, FORBES, https://www.forbes.com/sites/kevinmurnane/2017/05/13/how-to-protect-yourself-from-the-global-wanacry-ransomware-attack/#5d67649882dd (last visited June 1).