Why Should I Care About Privacy & GDPR?

Privacy is one of the most important human rights we have. GDPR demands a conversation focusing on data ownership and control.

By Matthew O. Fisch,

Senior Vice President &
Security Consultant, Towerwall

Towerwall
Protecting Data Integrity

Table of Contents

Why Should I Care About Privacy & GDPR?

Introduction	5
History of Privacy Rights and Protection of Personal Data	6
What is GDPR?	9
Definitions (GDPR EU Parliament, 2016)	14
Sources	16

About the Author

Matthew Owen Fisch

Senior Vice President &
Security Consultant, Towerwall

Matthew Owen Fisch is a Global Cyber Security Consulting and Sales Executive with more than Two Decades' Worth of Experience in high tech emerging markets.

Matt brings a visceral commitment and drive to customer success

Matthew Fisch is a dynamic and results-driven leader with a record of exceeding client expectations, building long-term relationships, and a strong record of success and team achievements. He currently consults with executives and clients to enable Cyber Security Forensic and Network optimization solutions which protects customer trade secrets, client information, and thus improves return on assets and revenue for stock holders. He possesses a deep and profound consulting expertise in stakeholder and ecosystem analysis, and pricing, and throughout an illustrious career, he has demonstrated a keen ability to assess customer requirements, and to discover compelling business problems with proposed solutions to engineers and C-level executives.

Matt has also traveled extensively to over 50 cities flying over 3M miles to engage with a global set of clients and to pursue diverse cultures and challenges.

matthewf@towerwall.com

Introduction

Privacy is one of the most important human rights we have. GDPR is essentially an enforcement of our right to privacy in the digital world. The creation of the GDPR regulation demands a conversation focusing on data ownership and control. Who owns the data and who controls it?

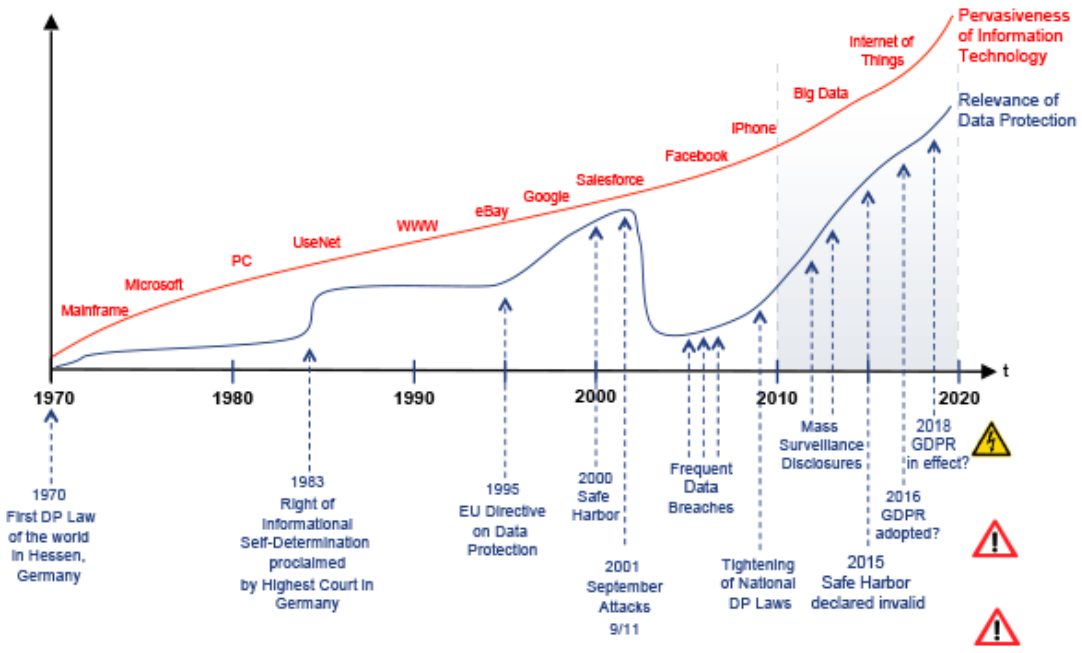
I am passionate about privacy, how it impacts our lives and our human rights. Our entire nation was built on human rights. People came to the US to embrace the freedoms spelled out in the original constitution and the 27 Amendments. Many remember stories from our grandparents that were passed on throughout the generations about the past abuse of human rights. Individuals came to this country ready to fight and defend the constitution to ensure personal rights. My father was a Purple Heart recipient and Army hero who fought in the "8th Army in 1951 in the Battle of Bloody Ridge (U., 2018)." Throughout his many military deployments, he observed many human rights violations. As a proud American, two of the grossest infringements were the violations of ***Habeas corpus*** and privacy.

Today Privacy is well defined in the bedrock of American Law. The proxy test consists of four elements:

- Right to be let alone
- Public disclosure of private facts
- Rights not to be depicted in a false light
- Commercial misappropriation of personal data

The importance of privacy may be best understood by examining the invasion of privacy in our daily lives? Think of invasion of privacy in terms of physical intrusions (i.e. planting secret recording devices) or informational intrusions (i.e. employer reading personal email for fun). Confidentiality, personal data protection, data encryption, data security, anonymity, and adherence to fair information practices create an informational dimension to privacy. Other dimensions of privacy include decisional intrusions (i.e. states banning assisted suicide), proprietary intrusions (i.e. advertisers using someone's photo without permission), associational intrusions (i.e. seeking membership in an exclusive club) and intellectual privacy.

In terms of the ubiquitous environment of information, we want **rights for protection of personal data and privacy.**



History of Privacy Rights and Protection of Personal Data

The Right to Privacy

The constitution of the US has no mention of the right to privacy. This gap existed until 1890. Privacy Rights first originated from the Law review called the “The Right to Privacy” (4 Harvard L.R. 193 Dec. 15, 1890) Authored by Supreme Court Justices Samuel Warren and Louis Brandeis. Building on foundational “laws of defamation, of literary property, and of eavesdropping,” Brandeis argued that the central, if unarticulated interest protected in these fields was an interest in personal integrity, "the right to be let alone," that ought to be secured against invasion (Louis Brandeis, 2018)”

Many more US privacy laws were spawned by the Warren and Brandeis’s law review including HIPAA (Health Insurance Portability and Accountability Act) instituted in 1996 to protect and secure Medical and sensitive PII, and GLBA (Gramm-Leach-Bliley Act 1999) which protects financial data.

Edward Snowden

After the attack of September 11, 2001, the US congress passed the Patriot Act, the Precise Act, and the FISA Amendment Act's PRISM surveillance program (mass surveillance in the US). This gave Federal Agencies more

flexibility to conduct surveillance and to enable more ubiquitous monitoring in order to address national security and terrorism issues. Edward Snowden made significant disclosures regarding these laws and accused Facebook of participating in the NSA PRISM surveillance program.

US Safe Harbor Agreement

In 2013 Austrian Lawyer Max Screms filed a complaint against Facebook with regard to prohibiting transfer of personal data from Ireland to the US in their cloud servers. On Sept 23, 2015 EC ruled in Schrem's favor, declaring the US "Safe Harbor" agreement invalid, and held that individual data protection authorities were permitted to suspend data transfers to third countries if they were in violation of EU. Subsequently, the EU Court of Justice ruled that Safe Harbor was invalid, partially because it did not provide legal remedies for citizens who wished to gain access to their data, have their data amended, or erased.

International Safe Harbor Principles

Challenges arose regarding the storage and transportation of data between countries, and "International Safe Harbor Principles (1998-2000) were developed in order to prevent private organizations within the European Union or United States which store customer data from accidentally disclosing or losing personal information. In 2015 Safe Harbor was overturned by the European Court of Justice (ECJ), which enabled some US companies to comply with privacy laws protecting European Union. "US companies storing customer data could self-certify that they adhered to seven principles, to comply with the EU Data Protection Directive (GDPR EU Parliament, 2016)." The seven principles of the commission include:

- **"Notice** - Individuals must be informed that their data is being collected and how it will be used. The organization must provide information about how individuals can contact the organization with any inquiries or complaints.
- **Choice** - Individuals must have the option to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security** - Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity** - Data must be relevant and reliable for the purpose it was collected.
- **Access** - Individuals must be able to access information held about them, and correct or delete it if inaccurate.

- **Enforcement** - There must be effective means of enforcing these rules. (GDPR EU Parliament, 2016)."

EU-US Privacy Shield Framework

US Secretary of Commerce Pritzker, and EU commissioner Jourova, announced the approval of the EU-US Privacy Shield Framework to comply with EU requirements for transferring data back to the US. (Kramer, J. J, Nov, 2107). They expanded the role of *US regulatory authorities including US Dept. of Commerce, the FTC, and the DOT*. EU-US Privacy Shield LAW Mandates the following requirements:

- Respond to complaints in 45 days
- Provide a response with assessment and solutions
- Provide information to the FTC when requested
- Cooperate with DPA (Data protection Authorities)
- Submit regular compliance reviews
- Enhance monitoring

The new framework details stronger responsibility for US companies to protect the personal data of Europeans and stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission. Through increased cooperation with European Data Protection, The Federal Trade Commission Act carries civil penalties of up to $16,000 per day for violations. If an organization fails to comply with the framework it must promptly notify the Department of Commerce, or face prosecution under the 'False Statements Act'.[15]

However, US President Donald Trump signed an Executive Order entitled "Enhancing Public Safety" which states that *US privacy protections will not be extended beyond US citizens or residents:*

> *"Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."*

Controversy - EU-US Privacy Shield

The European Commission has stated that The US Privacy Act has never offered data protection rights to Europeans. German MEP Jan Philipp Albrecht and campaigner Max Schrems criticized the new ruling, and many Europeans demanded a mechanism for individual European citizens to lodge complaints over the use of their data, as well as a transparency scheme to ensure that European citizens' data does not fall into the hands of U.S

intelligence agencies. As of February 2017, the future of the Privacy Shield is contested by Europe.

What is GDPR?

GDPR is the European Law that governs how your personal data is protected. The Regulation defines rules relating to the processing of personal data and the free movement of personal data. “It protects fundamental rights and freedoms of natural persons and their right to the protection of personal data.” There are 99 GPDR Articles that need to be examined for applicability to your business processes.

When does It Apply?

On 25 May 2018, the EU General Data Protection Regulation (“GDPR”) goes live. It is the biggest change to European data protection law in over 20 years, and will have a major impact on businesses across the USA and all around the world (Thomas J. Smedinghoff, 2017).”

What are the Stakes?

“Pursuant to GDPR Article 83, infringements of certain provisions of the regulation shall subject controllers and processors to administrative fines up to 20,000,000 euros, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Kramer, J. J., 2017).” “The maximum fine for breaching the GDPR is up to 40

times larger than under the previous law, and even more for big business (Thomas J. Smedinghoff, 2017)."

GDPR Development Project

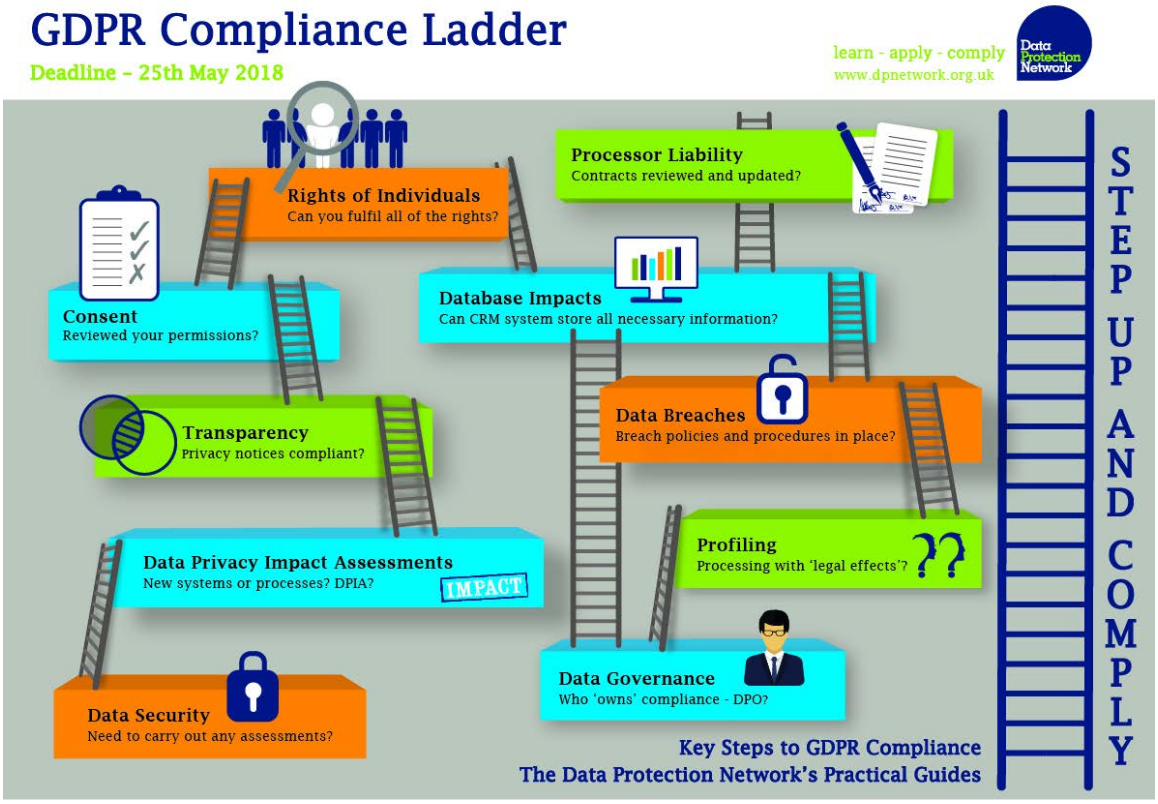
In response to the Edward Snowden disclosures, Europeans responded with the development of GDPR to supersede their current 95/46/EC directive. Their objective is to:

- Unify and align the multiple EU regulations into one
- Improve corporate data transfer rules outside the EU
- Improve the user control over PII
- In April 2016 the final Legislation was approved and the regulation becomes enforceable May 25th, 2018. GDPR will supersede the 95/46/EC directive.

GDPR Basis

Covered entities with EU employees or EU customers that are storing PII and managing PII data in transit must be compliant with GDPR. GDPR applies to the processing of personal data in the course of the activities of an establishment of a "controller" or a "processor" in the European Union, regardless of whether the processing takes place in the Union or not.

It applies offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects or the monitoring of their behavior as far as their behavior takes place within the (GDPR EU Parliament. (2016)." The European Country DPO (Data Protection Office) will examine the processing of data, the volume of data, the regularity of processing, and the profiling of data. *"The law applies to all processing of personal data inside the EU and personal data being sent outside the EU. The* ***GDPR will directly impact US higher education institutions*** *in terms of any processing of personal data of students travelling to the EU, students being recruited and accepted into programs from the EU, and employees or self-employed contractors (including academic staff) travelling to and from the EU, as well as academic research that includes the processing of personal data and is conducted in the EU or contains personal data that belongs to EU citizens (Tambellini Group)."*



GDPR requirement highlights for covered entities and processors (articles 1-99):

- Data Protection Officers –"You are required to designate a data protection officer (and the data protection officer has related obligations to their position, Articles 37-39(Kramer, J. J. (2017)" This can be an officer of the company or someone responsible for the management of the data or an outsourced appointed vCISO qualified in GDPR regulations and procedures.
- Reporting Data Breaches (Article 33 & 34) -Legally you are required to report a breach within 72hours. This includes Lost PCs with PII, Hacks, and violations of access authority.
- Higher Standard for Consent (Article 7 Right to withhold Expressed Consent)- You have the responsibility to offer explicit consent forms to holding data, and obligations to erase or restrict the use of PII data. You must explicitly send a request letter to be signed for consent to store and to process their data. This means that both Opt-In and Opt-Out clicks are insufficient.
- Implied Pseudonymisation of PII data - "The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to

ensure that the personal data are not attributed to an identified or identifiable individual (GDPR EU Parliament, 2016)."

In such a manner that the personal data can no longer be attributed to a specific data subject

- **Rights of Data Subjects** (Article 15 Right to Access, Article 17 Right to Erasure, Article 20 Right to Data PII Portability)- Individuals have a right to obtain copies of all their personal data you are processing, within 30 days. They will present you with a SAR (Subject Access Request), and you must provide individuals with extensive information about how you will process their data. "They also have the right to have it ported to another provider or to object to its processing on certain grounds, and may also be able to require its erasure – the "right to be forgotten" (Thomas J. Smedinghoff, 2017)."
- **Processors Now Liable (**Article 21 Right to Object to Processing for Controller and Processor, Article 18 Right to Restrict Processing, Article 28 Processor Requirements)- Under the previous law, if you processed personal data on someone else's instructions, you were a "data processor" and not a "data controller" and not directly subject to the law. This is no longer the case; data processors and data controllers are jointly liable for breaches they are involved in (Thomas J. Smedinghoff, 2017)."

Recommendations

GDPR does introduce both policy and implementation challenges with costs and severe non- compliance penalties. Therefore, senior management will want a cost/benefit analysis. Keith Wixler, head of legal council for Michelin in Lyon France, mentioned "GDPR will be a challenge, and especially for mapping business practices to the GDPR articles." According to Keith, it's a significant task that must be started now as they are already doing in Europe.

We recommend that you consider white-boarding your applicable business processes. Analyze IT Impact, and identify "***GDPR in-scope"*** personal data used that is mapped to a business process for customers and non-customers (Articles 30,13, 14 & 7). Moreover, we advise reaching out to Outside Council and a GDPR consulting firm who can perform a Data Protection Impact Assessment (DPIA) which includes a Risk Assessment , Gap Analysis, and Business Impact Analysis so you can understand your risk posture.

GDPR Enforcement ("Tricky Waters")

It is not an ostensible approach to just say that there are no precedents to GDPR and therefore no realistic enforcement. "Compliance with the GDPR is overseen by the national supervisory authorities and, for US entities participating in the Privacy Shield scheme, the International Trade Administration of the US Department of Commerce and the Federal Trade Commission (FTC), which can levy fines of up to $40,000 per day for non-compliance." An individual also has the right to redress in court if the supervisory authority fails to take adequate action. The GDPR includes several provisions that encourage the individual EU countries to adopt additional criminal sanctions for breaches, which means that a CEO of a US company found to be in breach may face criminal charges when stepping onto European soil (Tambellini, 2017)."

Do they have Jurisdiction here in the US? Can the FTC get involved?

(The below are open-ended questions the board should be asking and investigating with consultants and outside council)

- Exposures?
  Being located or Headquartered in the US ostensibly may not mean you have impunity nor are you necessarily shielded from the GDPR. The question "why do I care" is a fundamental matter of *basis* and a matter of *jurisdiction*, which in the case of GDPR has no case precedents. If one of your European clients or employees files a SAR complaint that you, "The Controller, " or your "Data Processor" have ignored the GDPR regulation or failed to respond to the SAR, then a European Country Protection agency can file a complaint. It's then possible that the European Country District Court could, ostensibly find you guilty of non-compliance and issue you a significant fine.
- US Federal Trade Commission Act Section 5 Risks?
  "Section 5(a) of the Federal Trade Commission Act (FTC Act) (15 USC §45) prohibits "unfair or deceptive acts or practices in or affecting commerce." This prohibition applies to all persons engaged in commerce, including banks. The Board has affirmed its authority under section 8 of the Federal Deposit Insurance Act to take appropriate action when unfair or deceptive acts or practices (UDAP) are discovered. If your company is making claims then FTC 15 USC §45 might apply (Unfair and Deceptive Practices)."

Jurisdiction is not just Physical Jurisdiction:

Your company could be headquartered in Rhode Island. You may have MA resident employees. If in fact, MA residents commute to your company or you are in any way managing MA residential PII on your website or database, then a MA resident ostensibly could file a complaint with the local Rhode Island Court. With basis a significant fine could be levied. In other words, in theory, through local Jurisdiction, there could be an enforcement path for GDPR non-compliance.

Other Remedies Under the GDPR: The Right to Judicial Relief

In addition to providing for the assessment of administrative fines, the "GDPR also authorizes data subjects to seek judicial relief against a supervisory authority, controller, or processor to obtain compensation for any damages. Judicial actions are without prejudice to any other administrative or non-judicial remedy under Articles 78, 79, and 82. In other words, the ability to bring an individual action for damages and compensation is independent from any action taken by a supervisory authority to impose administrative fines (Kramer, J. J., 2017)."

Definitions (GDPR EU Parliament, 2016)

- **Personal data** - Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- **Processing** - Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **Restriction of processing** - The marking of stored personal data with the aim of limiting their processing in the future;
- **Profiling** - Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict

aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

- **Pseudonymization** - The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- **Controller** - The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **Processor** - A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **Third party** – A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;
- **Consent of the data subject** - Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him…
- **PII**- Personally Identifiable Information is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data be considered PII Personal data breach' means a breach of security leading to the accidental or unlawful destruction; loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed "GDPR EU Parliament. (2016).
- **SAR** - Subject Access request
- **Attorney–client privilege** or lawyer–client privilege is a "client's right privilege to refuse to disclose and to prevent any other person from disclosing confidential communications between the client and the attorney (*Black's Law Dictionary*)

Sources

GDPR EU Parliament. (2016). *GDPR EU Parliament on protection of natural persons with regard to processing of personal data and on free movement of such data.pdf*. GDPR EU Parliament on protection of natural persons with regard to processing of personal data and on free movement of such data.pdf

Intersoft Consulting . (2017, December 20). General Data Protection Regulation GDPR. Retrieved January 2, 2018, from https://gdpr-info.eu/

Kramer, J. J. (2017, November 28). . GDPR, PART V: UNDERSTANDING THE FINES AND PENALTIES PROVISIONS . Retrieved January 2, 2018, from HTTP://LEWISBRISBOIS.COM/PRACTICES/DATA-PRIVACY-CYBER-SECURITY/BLOG/GDPR-PART-V-UNDERSTANDING-THE-FINES-AND-PENALTIES-PROVISIONS

Louis Brandeis. (2018, January 15). Retrieved January 20, 2018, from https://en.wikipedia.org/wiki/Louis_Brandeis

Louis Dembitz Brandeis (/ˈbrændaɪs/; November 13, 1856 – October 5, 1941) was an American lawyer and associate justice on the Supreme Court of the United States from 1916 to 1939

Mass surveillance in the United States. Retrieved January 2, 2018. (2018, January 2). Retrieved February 15, 2018, from https://en.wikipedia.org/wiki/Mass_surveillance_in_the_United_States

Tambellini Group . (2017). The European General Data Protection Regulation (GDPR) and Higher Education Institutions. *2017-GDPR-Report-Executive-Summary-Tambellini.pdf,* 1-6. Retrieved December 12, 2017.

Thomas J. Smedinghoff, T. (2017, November 7). GDPR - The “Great Data Protection Revolution” Less than 200 Days to Go. Retrieved December 9, 2017, from https://www.lockelord.com/newsandevents/publications/2017/11/~/media/035347F0F6284442A213EDEFC59E96C8.ashx

VII. Unfair and Deceptive Practices — Federal Trade Commission Act. (n.d.). VII. Unfair and Deceptive Practices — Federal Trade Commission Act. Retrieved November 12, 217, from https://www.fdic.gov/regulations/compliance/manual/7/vii-1.1.pdf
Federal Trade Commission ActSection 5: Unfair or Deceptive Acts or Practices

U. (2018, February 14). US ARMY Korean War Campaigns . Retrieved January 15, 2018, from https://history.army.mil/html/reference/army_flag/kw.html
https://history.army.mil/index.html

About Towerwall

At Towerwall we believe that a second set of eyes is crucial to your data security. Many vendors implement a “check list” mentality when tasked with assessing more than one business operation. Whereas, Towerwall uses proven methods for assessing risk, coupled with extensive experience to provide you with an actionable security risk assessment.

For nearly 25 years, Towerwall has helped scores of companies safeguard their data and leverage their investment in IT with advanced information security solutions and services. As a market leader within the IT security industry, we offer complete IT security services. By working together we can collectively lower the risk and cost of a data breach. Each passing day we come to see the stakes are getting higher, but more than good business practice, today’s state-of-the-art data security is the law. Our time-tested methodologies provide a consistent, repeatable, and measurable approach to information security.

774.204.0700 info@towerwall.com www.towerwall.com