

THE FUTURE OF TECHNOLOGY AND INNOVATION: A CULTURAL ANALYSIS OF
DATA REGULATION IN THE UNITED STATES AND FRANCE

Zoë Truong

TC 660Hs
Plan II Honors Program
The University of Texas at Austin

May 13, 2020

Deirdre B. Mendez
McCombs School of Business, Center for Global Business
Supervising Professor

Caroline A. Bartel
McCombs School of Business, Management
Second Reader

ABSTRACT

Author: Zoë Truong

Title: The Future of Technology and Innovation: A Cultural Analysis of Data Regulation in the United States and France

Supervising Professors: Deirdre B. Mendez, Caroline A. Bartel

Our ease of sharing and receiving personal and private information through technology has enabled an environment where individuals and organizations capable of articulating that data have the advantage in advancing technological progress. With the threat of increasingly invasive ways of capturing data and growing unease in organizations' abilities to protect personal information, many countries like France seek to improve public policy and regulation for digital environments, adding provisions to the already comprehensive General Data Protection Regulation from the European Union. The United States does not have a federal policy on data regulation, which has led to numerous difficulties and penalties for American companies operating in the European Union. This thesis aims to understand the different cultural tendencies and attitudes exhibited by French and American citizens that could help explain reasons for the state of cyber policy in both nations. Utilizing the Mendez, 2017 ARC System, this thesis will analyze personal interviews conducted with both French and American technologists as well as polls, panels, and academic journals that frame the current and past behaviors of French and American societies.

ACKNOWLEDGEMENTS

I would like to acknowledge my parents, Nguyen and Charles Truong, for affording me the opportunity to conduct the research in France for this thesis and providing love and support for all of my endeavors. I would also like to thank my brothers Tri and Minh for supporting me as well as without their presences this thesis would not have been possible.

I would also like to thank my advisors. Thank you to my supervisor, Professor Mendez, for guiding me through this paper and providing indispensable advice to keep me confident throughout the research and writing process. I would also like to thank my second reader, Professor Bartel, for her class and for offering valuable perspectives for my work, which helped develop the research into an enriching experience for me.

Finally, I would like to thank the Plan II Program for all of its support in making this thesis possible. Some of my most treasured classes and experiences throughout college are thanks to Plan II and I would not have had the confidence to start such a research project without all the guidance from the teaching and administrative faculty. A special thank you to my World Literature Professor Jerome Bump for being the most influential person to my thesis and my college career.

Table of Contents

Chapter I: Data Protection in the United States and Europe	1
Chapter II: Overview of US and French Views on Data Privacy	12
Chapter III: Overview of US Cultural Tendencies	16
Chapter IV: Overview of French Cultural Tendencies Crisis	23
Chapter V: Conclusions	32
Bibliography	35

CHAPTER 1: DATA PROTECTION IN THE UNITED STATES AND EUROPE

Data privacy concerns ran through United States media headlines throughout 2018 after the European Union (EU) fully implemented the General Data Protection Regulation (GDPR), which replaced the previous Data Protection Directive of 1995¹. While the prevalence of technology in society seemed to have driven most of the discourse, data privacy policies have existed for decades². However, different nations define the elements of security and personal data with varying degrees of severity. This paper will focus specifically on the United States and France, with consideration of the latter's membership in the European Union. These two nations were chosen for case studies given various motivations for the strong positions members of both societies take in the data policy conversation. These motivations will be explored later in the paper.

¹ Denise Lebeau-Marianna, *Data Protection Laws of the World*, 2, January 23, 2019, accessed October 18, 2019, <https://www.dlapiperdataprotection.com/index.html?t=law&c=FR>.

² Priscilla M. Regan, Gerald FitzGerald, and Peter Balint, "Generational Views of Information Privacy?," *Innovation: The European Journal of Social Sciences*, 81, <https://doi.org/10.1080/13511610.2013.747650>.

Data Protection in the United States

The United States is particular about what type of personally identifiable information (PII) is qualified for protection. As a result, US data policy is distinguished from European data policy in that there exists regulations aimed at defined sets of PII. In general terms, there are laws that protect US citizens' medical and educational informations, privacy when underage, and financial records to name a few³. Health Insurance Portability and Accountability Act (HIPPA) covers the medical side, Family Educational Rights and Privacy Act (FERPA) for students and parents, but in general the US did not have data privacy regulations quite like some of the European Union's later policies in the 1990's and 2010's. Instead, individual states—in particular, California—enacted its own privacy laws in the absence of federal protection. In 2002, years after Europe had substantiated privacy concerns with the Data Protection Directive of 1995, California passed laws specifically pertaining to data breach notifications. These notifications will be explained in further detail under the European privacy law section as there is a greater measurable impact in the EU across a greater number of people than there is in the US. But, it is important to recognize that the California laws underscored an aspect of information security that had not been approved by any European legislation up until the GDPR. Despite the lack of US-wide legislation, California's attempt to address the burgeoning technology information sector was unique and influential for the European Union⁴.

³ Jay P. Kesan, Carol M. Hayes, and Masooda N. Bashir, "A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy," *Indiana Law Journal* 91, no. 2 (Winter 2016): 278, <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=113199291&site=ehost-live>.

⁴ Determann, "Social Media," abstract, 5.

Data Protection in Europe

European Union

In order to examine rulings on any data privacy violations in France, there must first be explanation of the European Union policies that serve as a basis line for these decisions. Much of the framework that makes up the GDPR finds its genesis in the EU's Directive. The Directive, implemented in 1995, was a comprehensive piece of legislation that outlined the transfer of personal, sensitive data in and out of the EU. It set the standards for data protection and delineated a multitude of dimensions for what categorized as sensitive data⁵. With new restrictions in place in Europe, nations like the United States had to reach further agreements or develop new policies to be able to obtain data from any EU citizens⁶. As of 2016, the modern day law upheld by the EU is the GDPR. Unlike its predecessor, the GDPR takes more "restrictive" stances on what constitutes personally identifiable information (PII) and how that information is processed⁷. Areas of society or business that are not directly covered in the GDPR are up to interpretation by the Member States to enact their own regulations, if deemed necessary⁸.

⁵ Müge Fazlioglu, "Beyond the 'Nature' of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States," *Fordham Urban Law Journal*. 46, no. 2 (April 2019): 280-281, <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=136193122&site=ehost-live>.

⁶ Samantha Cutler, "The Face-Off between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information," *Boston College Law Review*, 1516-1517, <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=129454710&site=ehost-live>.

⁷ Lebeau-Marianna, *Data Protection*, 2.

⁸ Lebeau-Marianna, *Data Protection*, 3.

In order to identify mishandling of security protocols amongst GDPR-affected organizations, the EU defined specific roles to highlight groups or individuals that are responsible for overseeing the transfer of data. These three roles, with higher authority levels available for specific positions, are the supervisory authority, controllers, and processors. Each nation essentially has its own supervisory authority. This is a group of individuals or delegates that ensure that the laws are being applied and all guidelines are followed well⁹. For France, this group is known as the Commission Nationale de l'informatique et des Libertés, or CNIL. At an organization level, businesses maintain positions for one or many controllers and processors. The controllers identify meaning in the personal data being handled by the organization, deciding how that data should be managed. The processor carries out the commands of the controller. The GDPR puts greater emphasis and responsibility on the controllers, even if the processing was done through some form of automation¹⁰.

The impact that these new sets of guidelines have had on the Member States and the rest of the world is already apparent in the first year since the GDPR's full implementation. Two performance metrics that measure the legislation's effectiveness in creating a fair, well-regulated environment for data transfers are the number of breach notifications and the fines placed on corporations. While the latter isn't necessarily a mark of how well the laws work, the fines do showcase that the delegated authorities are actively monitoring organizations' management of personal data. Breach notifications are initiated by an organization's controller and carry up to

⁹ Lebeau-Marianna, *Data Protection*, 3.

¹⁰ Fazlioglu, "Beyond the 'Nature,'" 276.

the supervisory authority. These organizations must take discretion into whether or not the potential data breaches included any impactful PII¹¹. In addition to measuring the magnitude of the breach, organizations also have strict time frames in which they must report the information to the supervisory authorities¹². This heightened sense of urgency in breach notifications explains the 742 breach notifications submitted for review by the CNIL from the time of the GDPR's implementation and the first of October — a fourth-month period. These notifications involved over 33 million French citizens¹³, but there is doubt as to whether the influx of notices were genuine cases or merely cautious actions. The distribution of the type of data breach is seen in Figure 1, with the highest offender being a breach of confidential data. Some organizations feared consequences if they didn't report the potential breaches, which has critics of the GDPR unsure of whether the framework is actually performing or if it merely floods CNIL with false cases¹⁴.

¹¹ "Breach Notification," DLA Piper, last modified January 23, 2019, accessed October 18, 2019, <https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=FR>.

¹² "Breach Notification," DLA Piper.

¹³ "Violations de Données Personnelles : 1er Bilan Après L'entrée en Application du RGPD," last modified October 16, 2018, accessed October 18, 2019, <https://www.cnil.fr/fr/violations-de-donnees-personnelles-1er-bilan-apres-lentree-en-application-du-rgpd>.

¹⁴ Philipp Schröder-Ringe, "The Amount of Data Breach Notifications in Germany and Europe Exploded since 25th May 2018," Härting, last modified September 20, 2018, accessed October 18, 2019, <https://www.haerting.de/neuigkeit/amount-data-breach-notifications-germany-and-europe-exploded-25th-may-2018>.

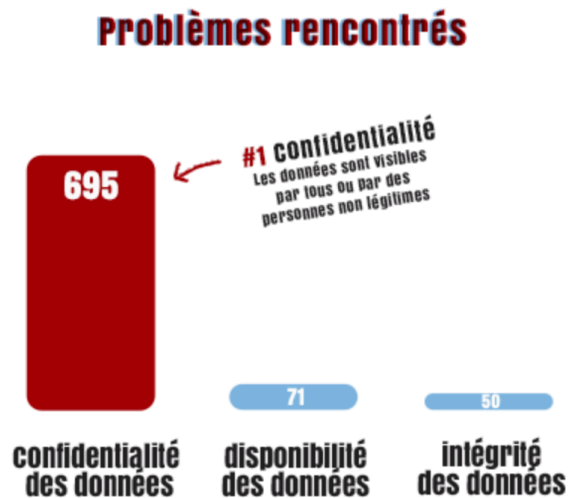


Fig. 1, Problèmes Rencontrés, illustration, CNIL, October 16, 2018.

Another key metric being mentioned alongside the GDPR is the financial impact on large corporations in violation of any of the terms of the law. The inundation of the breach notifications to supervisory authorities should have served as an omen to corporations that had not reorganized their information collection processes to ones that are GDPR-compliant. After the two-year grace period, the European Commission — the executive branch of the European Union — investigates organizations that are not aligned with the GDPR’s guidelines. Any violation from overdue breach notifications, lack of transparency of data processing, or improper security measures could warrant fines totaling thousands of dollars. The first organization to receive a GDPR fine was an Italian political party platform¹⁵. The charge was imposed by Italy’s supervisory authority, Garante, citing that the platform had not ameliorated known security problems that were brought to light during the GDPR’s grace period.

¹⁵ Kit Burden, "EU Update," *Computer Law & Security Review* 35, no. 4 (August 2019): 481, <https://doi.org/10.1016/j.clsr.2019.06.005>.

While that incident marked the first instance of the EU's strict stance on transparent technological processes, it is the subsequent investigations and fines on US corporations that fell into the spotlight through the first year of the regulation's implementation. Spurred by an activist group within the EU, the Commission turned its attention to the companies that are commonly referred to by the moniker, the Silicon Valley Technology Giants. Spanning several technology industries, companies like Apple, Google, and Facebook fall under this Silicon Valley umbrella. Some of these tech giants debuted during the nascent years of the telecommunications and information age, lasting through the decades to be the market leaders of their respective industries. At the same time, their abilities to stay relevant and innovate through the years is largely in part to the mass information collection from their millions and billions of daily users. For companies like Facebook, it is more apparent that PII is constantly flowing as data transfers across international borders. Google amasses location data from users to improve the accuracy of its proprietary map technology. Companies like Apple analyze the functions of its phones, laptops, and other devices to track anomalies in technological performance for future hardware and software updates. The extent to which the public understands the information provided to these corporations was often not challenged, at least not to the degree where any significant steps were taken by the US governing bodies to alleviate privacy concerns. However, after the attention to the information collection was brought to the European Commission, "extremely high-fines — up to 4% of annual global turnover"¹⁶ were levied on the tech giants.

¹⁶ Kyle Petersen, "GDPR: What (and Why) You Need to Know about EU Data Protection Law," *Utah Bar Journal* 31, no. 4: 12, <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=130821070&site=ehost-live>.

France

While the majority of what constitutes pertinent data privacy policy has thus far been explained by the General Data Protection Regulation, France was isolated as a country for comparison against the United States due to the European nation maintaining more robust data privacy laws compared to other EU members. As explained, the GDPR is a thorough set of legislation, but it does not cover every possible definition of data privacy throughout every industry of the EU. Instead, areas needing clarification could be spearheaded by the member states at their own discretion¹⁷. Many nations developed laws that harmonized with the GDPR guidelines to ensure there were no discrepancies in the fine lines. France was one of those nations, updating its own Decrees later the year of the GDPR's full implementation but added on stricter provisions to further protect data on health care and children¹⁸.

However, even prior to the GDPR, France was willing to question the US tech companies on their data usage. While French law was later updated to coincide with GDPR laws, the existing Decrees on data privacy applied across France and were robust in enforcement. For example, the CNIL requiring digitally processed medical PII go through preliminary authorization before use in medical research¹⁹. In 2013, CNIL had issued warnings and pending fines on Google for its

¹⁷ Lebeau-Marianna, Data Protection, 2.

¹⁸ Bart Custers et al., "A Comparison of Data Protection Legislation and Policies across the EU.," Computer Law & Security Review, <https://doi.org/10.1016/j.clsr.2017.09.001>.

¹⁹ Jeanne Bossi, "European Directive of October 24, 1995 and Protection of Medical Data: The Consequences of the French Law Governing Data Processing and Freedoms," European Journal of Health Law 9, no. 3: 202, <https://doi.org/10.1163/157180902760498742>.

lack of action in resolving a process-oriented issue with its management of personal data²⁰.

While France was not the only nation imposing fines on Google, it was the first to involve the supervisory authorities and lead the charge through the investigations. At the time France was only capable of imposing fines of up to 150,000 Euros, with potential to expand depending on how the court defined the infractions. Those actions by CNIL signify some united effort by the French supervisory authorities and potentially even the French government in support for robust data privacy laws. Despite being a member state of the EU, the individual actions by France showcase distinct protections for informed technology users. This situation is one of several instances that exemplify differences between France and the US regarding their perspectives on this digital regulation.

Looking to current cases of policy implementation from France, litigations initiated not by the CNIL but by an independent French organization point to additional instances of independent thought in data privacy regulation by the country. One of the activist groups that heavily scrutinized Facebook for its potential violations of GDPR law was a French NGO called the Internet Society²¹. This organization identified seven offenses pertaining to three of Facebook's applications: Facebook, Instagram, and WhatsApp, aiming at the controllers of the different branches of the corporation. It is important to recognize that the grievances set forth by this organization are not in conjunction with the CNIL. According to the terms of the GDPR, the

²⁰ Sam Schechner, "Corporate News: France Turns Screw on Google Data Use," in Factiva, previously published in The Wall Street Journal, September 28, 2013, <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=90446174&site=ehost-live>.

²¹ Kit Burden, "EU Update," *Computer Law & Security Review* 35, no. 1 (February 2019), <https://doi.org/10.1016/j.clsr.2018.12.007>.

Internet Society has the option of appealing to the French high court for further due processing if Facebook does not respond to the claims put forth by the French organization²².

While it is more difficult to characterize exactly what the EU focuses on in terms of information collection — besides fairness for all individuals affected by the tech economy — there is a minor emphasis on the rights of individuals for French interpretations and enforcements of these privacy laws²³. This is evident from French specifications of Data Privacy Impact Assessment-type responsibilities for controllers identifying data breaches. Data Privacy Impact Assessments are defined as “the process[es] that one goes through to determine if personally identifiable private information is being appropriately safeguarded.”²⁴ While France’s data policy acts don’t necessitate PIAs be created by controllers, they delineate a similar process of risk mapping for affected individuals²⁵. This is a unique aspect of the country’s privacy policies that is not listed in any other member states’ provisional laws.

All analyses on the EU’s regulatory bodies and policies were necessary for setting up discourse for observations of French information technology laws. While France may have unique perspectives and motivations for pursuing litigation against American businesses, it is the evolution of technology that should be kept in mind throughout this report. When considering the

²² Burden, "EU Update".

²³ Custers et al., "A Comparison".

²⁴ Laura Taylor, "Chapter 13 - Conducting a Privacy Impact Assessment," ScienceDirect, <https://doi.org/10.1016/B978-159749116-7/50018-4>.

²⁵ Custers et al., "A Comparison".

sheer market share that the tech giants have across many daily internet interactions consumers have, it can establish high barriers to entry into the markets as well as weaker power for individuals to seek alternative services. The ability for French companies to gain any meaningful competitive advantage against US corporations could be enhanced with a fairer access to information and safeguarding of an individual's rights to privacy. In interviews I conducted with French startup CEOs and investors, it became apparent that innovation in Europe is a strong goal ahead of the European Union alongside proper regulation of personal data. Whether or not those two goals can be concurrently accomplished is a question that is worth exploring outside of this thesis.

CHAPTER 2: OVERVIEW OF US AND FRENCH VIEWS ON DATA PRIVACY

Naturally, citizens' perspectives in both the US and France are diverse when it comes to data privacy. While data breaches have the capacity to impact everybody, the degree of that impact depends on the sensitivity of the information released. Financial data and health related information are among the most critical personal information people would seek to protect. The type of data most commonly shared is personally identifiable information typically sourced from technology that individuals interact with every day. Sources include a wide variety of websites, applications, and services across multiples lines of business. In order to analyze if culture has any influence on US or French views on data privacy, the cultural tendencies that are potentially relevant will be examined in light of the Mendez, 2017 ARC System cultural framework.

Before any of the cultural tendencies can be analyzed, there must be clear descriptions of the varying views on data privacy and their relationships with innovation. For the purposes of this analysis, all types of sensitive data will be grouped together. However, it is important to understand that individuals may have different opinions depending on the degree of sensitivity of the data, such as health, financial, and personal data. Going into each type of sensitive data is beyond the scope for this thesis but it is worth additional research.

To narrow the scope, this paper will only analyze these tendencies in two areas: personal habits and business settings. Since nationwide cyber policy is the type of policy discussed here and data privacy in daily life is deeply intertwined with digital business interactions, the goal of this study is understanding tendencies that are demonstrated by business entities. Businesses can help drive

decision making on the government level. However, data privacy is both a private and public interest. Attitudes towards both types of public policy can be a result of attitudes towards the technology in general.

The ARC cultural framework establishes eight cultural dimensions: *clarity, emotion, status, involvement, collaboration, authority, action, and organization*²⁶. Not all dimensions will be applicable for the topic, so the most relevant dimensions have been isolated to assess differences in attitudes demonstrated by the comments of French and American interviewees. These are the involvement, collaboration, and action dimensions.

There are a number of ways that the following cultural dimensions apply to the ideas of data privacy and security. Identifying interviewees' tendency for each dimension on data privacy may point to specific decisions in cyber policy.

The involvement dimension describes the level of interpersonal involvement among individuals and businesses and spans a range of two cultural tendencies--Network and Process orientations²⁷. Network-oriented individuals invest considerable amounts of time developing relationships, valuing high levels of trust. Process-oriented individuals take transactional views of business, limiting the degree of information shared with one another but quick to develop relationships. In

²⁶ Deirdre Brown Mendez, *The Culture Solution: How to Achieve Cultural Synergy and Get Results in the Global Workplace* (Boston, MA: Intercultural Press, 2017).

²⁷ Mendez, *The Culture*, 93-99.

terms of personal data privacy, the tendency for developing relationships could be valuable in understanding perceptions of relationships developed online.

The second cultural dimension considered will be the collaboration dimension for instances of responsibility²⁸. The collaboration cultural dimension describes a range of behavior from independent to group cultural tendencies. Independent-oriented people take individual responsibility and receive credit for their actions as individuals. Both wins and losses are personal responsibilities and characteristic of independent cultural tendencies. Group-oriented people tend to make decisions based on group consensus and subsequently receive the credit or blame as a whole. Independent-oriented cultural tendencies seem to be largely represented by ideas of personal data privacy as whole. Efforts made towards protecting ones personal data or at least being conscientious of it is something that can be associated with the idea of individual responsibility. Additionally, independent-oriented legal environments can facilitate opportunities for individuals to protect their own rights. Collective responsibility would have more protectionist or interventionist support on the business and government level. These cultural tendencies could be attitudes in support of the group collective as a necessity to create a proper innovation-forward environment in the digital world.

²⁸ Mendez, The Culture, 101-107.

The final dimension for consideration is the action dimension²⁹. This dimension spans a range of cultural tendencies from opportunity to thoroughness. Opportunity-oriented people move quickly to capture new opportunities as they arise and tend to not reflect on past engagements. Change is an inevitable existence and should be valued, especially when that change is innovation.

Thoroughness-oriented people are more comfortable making decisions once extensive research is conducted on specific situations. Always considerate of previous choices and any potential future opportunities, these individuals view change as disruptive and instead favor tradition. In the realm of business and invention, the action dimension can be apparent through a society's tendencies to value and embrace new opportunities. The opportunity tendency correlates with technological innovation. Attitudes that reflect this tendency are ones that prioritize innovation, possibly at the expense of legal protection. Any level of fixation or drive to prioritize these ways of business could be indicative of more opportunity-oriented individuals and societies.

These indicators were defined through observations, conversations, and interviews with individuals from both countries, but there are a multitude of considerations about the audience. Especially in the case of the cultural tendencies pulled from French culture, most of the analyses come from Parisian residents. While observations were made for residents from the Alsace region as well, all interviews were conducted in the Île-de-France, so the opinion may not be representative of other regions. Similarly, all US interviews were conducted in Texas. The same caution to regional differences applies in this space as well.

²⁹ Mendez, *The Culture*, 117-124.

CHAPTER 3: OVERVIEW OF US CULTURAL TENDENCIES

This chapter analyzes US cultural tendencies and the ways these cultural tendencies play a part in how American citizens view personal data privacy and cyber policy. Personal observations on US cultural orientation come from living a life in the United States. For the topics of business and personal data there were interviews conducted with US-based technologists, professors, businesspeople, and students that aimed to collect attitudes and sentiments towards technology, innovation, and cyber policy. The interview research was conducted between November 2019 and April 2020 and the conversations were based off the most pertinent information available concerning the General Data Protection Regulation and relevant policies.

Cultural Characteristics of the United States

The following figure is a generalized overview of US cultural orientation according to Professor Deirdre Mendez’s ARC System. For the purposes of relating to the analysis, only the involvement, collaboration, and action dimensions were measured and shown. This overview is based off of the interviews from Texas-based US citizens, observations mostly from the South with personal observations from travel in the Northeast, West, and Southeast, and a variety of survey data available on the topics of personal data privacy, business, and culture.

The generalized overview is represented in Figure 2, below.

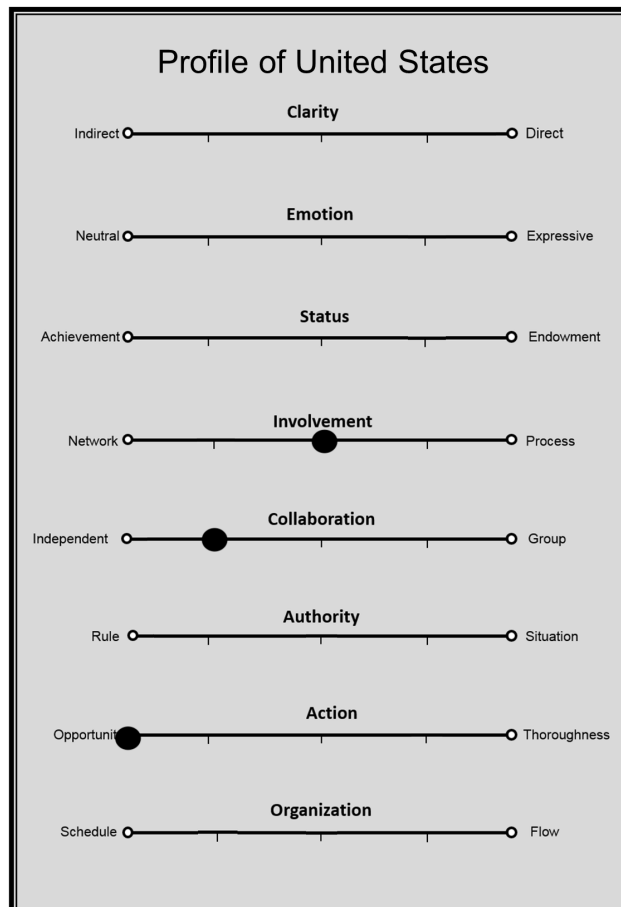


Fig. 2, Profile of United States, illustration.

Data and Interviews

In contrast to the research on France, there was less emphasis placed on personal interviews for the US-based cultural analysis as there were more readily available survey data and opportunities for observation on an academic and personal level that could help identify and isolate areas for research.

US Interviews Relating to Data Privacy

The information collected from the US interviews comes from US-based technologists and academics and addressed topics covering innovation, business, and regulation. Questions were asked of the US-based technologists on the future of personal data privacy and the role companies play on data protection, as well as topics on the impact of GDPR-type regulation for US businesses. The generalized overview profile of US individuals captures the results of the interviews, especially on the involvement, authority, and action dimensions.

Discussions surrounding personal data privacy with US technologists indicated more of an opportunity orientation. One interviewee took a stance that from a generational viewpoint, the younger digital generation is unconcerned with data privacy. Emphasizing the “freemium” model that many digital markets offer, the interviewee posits that existing social relationships help reinforce the intent to release even more PII for companies to use. A similar sentiment was taken by another interviewee, Professor Russ Finney, stating that this was a “mindset of acceptance”³⁰ and that the presence of successful software and technology like Facebook or the iPhone is

³⁰ Russ Finney, interview by the author, Online, Arlington, TX, April 10, 2020.

helped in part by this acceptance. These statements suggest to opportunity-orientation tendencies as they express an appreciation for the benefits of innovation and little caution or concern for consequences. On a public policy level there are definite cases in the more unstructured approach to US privacy laws considering the lack of strong US-wide policies on the basis of PII. With the standards set on a government level, there seems to be influence on individuals to approach personal privacy itself in a more unstructured way as well. In all interviews, the US-based technologists felt that there was more responsibility on the user for setting boundaries on the company's use of data. This stance regarding the responsibility of the individual speaks to the independent-orientation of the collaboration dimension.

There were some conflicting stances on questions concerning intrusive business practices that could potentially infringe on individual rights and personal information. One interviewee used the language that company policy outweighing private interest was “unfair” and supported European efforts that protect the right of the individual³¹. Four out of the six interviewees expressed a belief that rights of the individual are rising in importance compared to the responsibility of the individual. We currently still see attitudes that US individuals have full buy-in into invasive business practices for data as there isn't a motivation to get out “until something bad happens.”³² However, Pew research and other attitudes suggest that there is a growing proactive consideration on whether individuals can still exercise full rights to their data when it comes to corporations and business. In the case of governments, around 81% of US respondents

³¹ Interview by the author, McCombs School of Business, Austin, TX, March 6, 2020.

³² Finney, interview by the author.

indicated feeling a lack of control over collected data and around 79% expressed a form of concern of how the data is being used³³. The independent-oriented cultural tendencies like the sense of personal responsibility may be valued more strongly than opportunity-oriented and rule-oriented tendencies. This could indicate that US individuals are against instances of procedures and processes that could affect the individual right to manage one's own PII.

Relevant Histories Pointing to Current Biases

The United States is a relatively young country compared to France. Its short history could explain why there are less instances of thoroughness cultural tendencies in American society, as there are not centuries worth of tradition to value. However, the ethos of the American Dream is one tradition that suggests long-standing values for opportunity-oriented cultural tendencies as individuals expect and hope for a different economic future through personal achievements³⁴. Americans have strong optimistic attitudes for attaining opportunities and this positive outlook has continued throughout the country's short existence. There are a combination of factors that continue to buttress this ethos in the hearts of many Americans, and one major factor is the government and its actions to promote the ideology.

From a societal viewpoint, the threat of economic inequality is a strong motivator to support government efforts to develop economic or political policies that "enhance opportunities to advance in the labor market, such as policies that expand access to education and/or address

³³ Brooke Auxier et al., Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, November 15, 2019, <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

³⁴ Richard Nadeau, Vincent Arel-Bundock, and Jean-François Daoust, "Satisfaction with Democracy and the American Dream," *Journal of Politics*, <https://doi.org/10.1086/703070>.

inequities in the workplace.”³⁵ The belief for opportunity not only maintains the American Dream ideology but it also translates to a society that thus values individual achievements in innovation and business in general. This suggests that innovation is largely perceived as positive change that can promote socio-economic mobility and is fostered by policies from the state. One leading example of this is the emphasis and support of robust patent laws. The United States displays strong independent-orientated cultural tendencies by giving citizens opportunities to protect intellectual property and defend it in the court of law. Another example of how US society values achievements in innovation is the existence of the Silicon Valley, often associated as the breeding grounds for technological innovation and perceived to be an opportune incubator environment. How many of these businesses and organizations maintain such constant innovation is often through the means of data collection. While US federal policies are overall cognizant of the right to privacy, there are strong independent-oriented tendencies that suggest that the decision for personal privacy is more supported than an inherent right to privacy³⁶. This explains the growing number of “freemium” model businesses, which are common models for many online social media organizations or other personal technology. The freemium model is dependent on the use of individuals’ PII to improve the technology and make the overall experience more personalized for the end users. This creates stronger instances of network-oriented tendencies to support opportunity-oriented cultural , where end users hope that time and data spent towards using a technology will ultimately bring about positive change for the user experience. There’s a clear value in building these digital relationships by sharing information

³⁵ Leslie McCall et al., "Exposure to Rising Inequality Shapes Americans' Opportunity Beliefs and Policy Support," Proceedings of the National Academy of Sciences of the United States of America, <https://doi.org/10.1073/pnas.1706253114>.

³⁶ Kesan, Hayes, and Bashir, "A Comprehensive," 277.

that is very unique to the modern day technological environment. However, the discourse over the last decade seems to suggest that Americans are not as optimistic on the breadth of information being utilized by the government and other organizations³⁷. It is possible that US values are beginning to shift towards more process-oriented tendencies as users' trust towards organizations declines in the wake of several major data breaches over the last decade.

Companies like Equifax, Yahoo!, and Target have demonstrated that allowing organizations to control so much personal information comes at high risk of exposure through the work of highly-skilled hackers³⁸. For the most part many of these data breaches, while highly criticized by the media and affected individuals, was not followed up with stricter policy pressure from the US government. While politicians shared sentiment that efforts towards stricter cyber policy would be a necessary measure, the reality is that there still does not exist a comprehensive set of data protection regulation similar to the GDPR. Even while individuals express growing concerns on their data privacy, the growing indicators of process-oriented tendencies from Americans is not being reflected in US policy. This could be the case where the American political environment for independent-oriented tendencies no longer aligns with personal privacy that some Americans are seeking. Instead, the American political environment is potentially showcasing group-oriented tendencies that sacrifice the personal rights of individuals in order to maintain the perceived public interest in business and innovation.

³⁷ Auxier et al., Americans and Privacy.

³⁸ "The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information," Duke Law Journal, 556, Academic Search Complete (133418287).

CHAPTER 4: OVERVIEW OF FRENCH CULTURAL TENDENCIES

This chapter analyzes French cultural tendencies and their part in how French nationals view personal data privacy and cyber policy. A large portion of the analysis concerning French cultural tendencies is based on first hand observations and interviews with French students, teachers, technologists, and businesspeople from Paris. This research was conducted between the months of February and May of 2019 and the conversations were based off the most pertinent information available concerning the General Data Protection Regulation and relevant policies. Additionally, some data comes from attendance at panels held during the 2019 Viva Tech Conference at the Paris Exposition Center.

Cultural Characteristics of France

The following figure was constructed using the ARC System cultural framework and data collected from the interviews with the French nationals. This diagram shows a generalized overview of the cultural tendencies described in conversation on the topics of technology, business, and cultural insights. As with the US-based profile, for the purposes of relating to the analysis, only the involvement, collaboration, and action dimensions were measured and shown. The high level summary is represented in Figure 3, below.

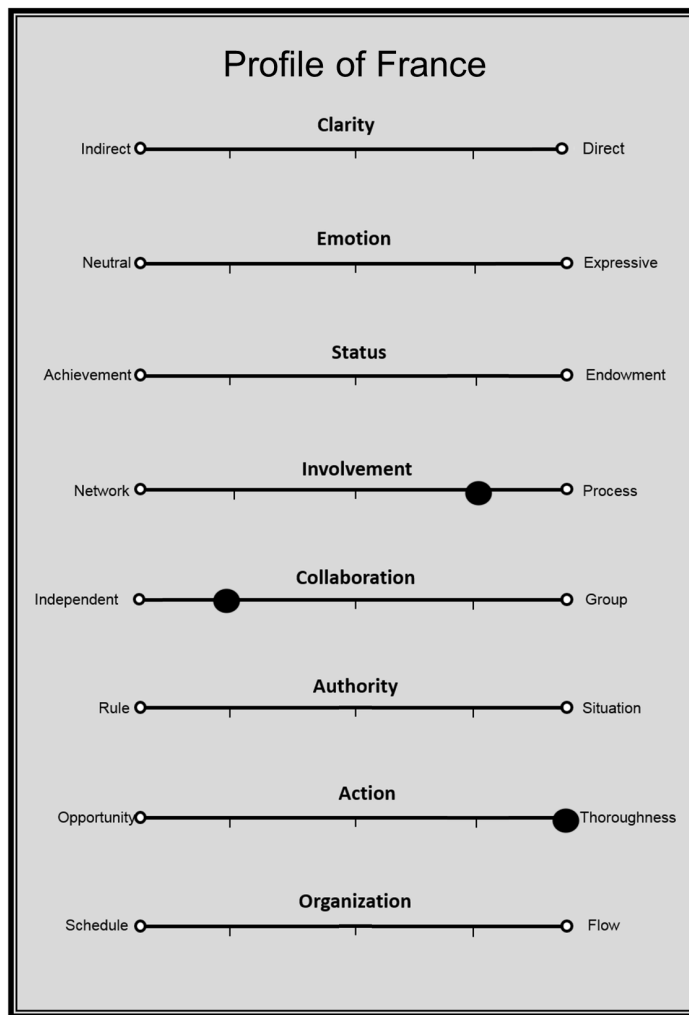


Fig. 3, Profile of France, illustration.

Data and Interviews

First observations for discussion are the data collected from the panels. The panels attended included the following titles: “Who Are the Future European Champions: Scaleups or Corporates,” “Is Regulation Fostering Innovation?; Innovation in Europe - Making It Happen,” and “AI for All: Private Companies, Public Good.”

Viva Technology Interviews and Relevance to Business and Data Privacy

The information collected from the “Innovation in Europe - Making It Happen” panel produced numerous instances of meaningful information regarding stances taken by the European Union, which is a nuance in the discussion of cultural tendencies that can’t be captured from the conversations with French nationals. Found in the panel discussion are instances of verbiage that can be representative of cultural tendencies found on the authority, action, and organization dimensions. The panelists were all members of the European Commission. This was an ideal opportunity to observe stances taken by the Executive Branch of the European Union, as the Commission is responsible for executing decisions put forth by the European Parliament and the Council of the EU — which makes it a key player for the concerns of the GDPR³⁹. Of the European Commission were three panelists: Pierre Moscovici, the Commissioner for the Economic and Financial Affairs; Carlos Moedas, the Commissioner for Research, Science, and Innovation; and Magrethe Vestager, the Commissioner for Competition. It is important to note that this panel conveys the stance of the European Union as a whole rather than France. Although French culture is the focus for this section, it is not possible to discuss perspectives of the French

³⁹ "European Commission," European Union, https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en.

on supra-national directives. As previously discussed, there are definite opportunities to highlight French preferences and decisions for more robust policies, the observations from the panelists are only meant to highlight opinions from the European Commission alone.

Discussion that had strong tendencies in the action dimension were mostly made by Commissioner Vestager. She addressed topics on the viability of regulation in the digital economy and its impact on Europe's ability to be innovative and attract European talent to the digital space. Her discussions on regulation revealed stances that had strong thoroughness orientations. While Vestager made concessions towards the idea that competition was a "driver of innovation", she was careful to express that regulation as a whole is a strength. This is indicative of a thoroughness orientation because of her explanations on how regulation can be effective. Thoroughness involves tendencies to make specific and careful strategies through reflection. Vestager takes stances that unregulated markets can lead to monopolies and the innovation isn't always good. Although the title of the panel would lead one to believe that innovation in general was a major goal for Europe, there were strong tendencies to put out ideas where innovation was positive and then reel back and consider instances where innovation-narrowed drives have the potential to be harmful. The panel would clearly discuss innovation and regulation as a complex issue that always included opportunities and inequalities. Additionally, there was a fairly distinct attitude towards accountability in business environments that can be interpreted from Vestager's comments on market freedom and opportunity. While accountability tends to be on a smaller scale, the same sense of calculated and intentional work that aims to be fair has strong thoroughness-orientation.

Later on in the panel was discourse on the corporate taxation by the various European supervisory authorities and the European Commission. The main panelists covering the taxation were Pierre Moscovici and Carlos Moedas. Part of what made the GDPR a hot-button topic was the prevalence and magnitude of fines of multinational businesses⁴⁰. In response to the role that the regulation played in competitiveness, Moscovici often frames the taxation as a means for digital competitiveness. Besides the fact of the matter that the gravity of the fines are meant to send a message about the GDPR's importance to the EU's competition and innovation goals, there is a message that taxation is aimed at being inclusive. Again, the commissioners relate the topic to a sense of inequality and the need for actions to promote fairness, with Moedas clearly stating that "innovation is fairness" in response to the potential of digital taxation inhibiting entrepreneurs that aim to join the digital space. This sort of statement embodies the thoroughness-orientation as seen from Commissioner Vestager's comments. The EU aims to avoid protectionist labels and instead finds the efforts to diminish inequality in the digital space outweigh the supposed damage to multinationals.

According to my interviews with French nationals, the sort of cultural tendencies inferred from the interviews indicated that oftentimes French attitudes were not starkly different from similar behaviors in the United States, the behaviors being regulation of business. Questions were asked of the French nationalists on the future of personal data privacy and the role companies play on data protection, as well as topics on the impact of regulation like the GDPR for French business.

⁴⁰ Petersen, "GDPR: What," 1.

The language used by the French nationals seemed to mirror elements of the United States strictly on topics of business. In general, people in industry and entrepreneurs alike observed that GDPR-restrictions were strong. The language used to describe these policies were more negative in nature. The words “strict” and “unfriendly for startups” appeared in one interview, yet in the same conversation these affirmations were countered with statements that culturally Europeans are “more aware of these regulations”⁴¹ and that the policies “[calm] everyone down.”⁴² Again, there is a strong sense of thoroughness-orientation as interviewees found the processes as a natural effect of operating in the EU and that innovation comes from working with those restrictions to still reach the same level of competitiveness that is often idealized in US markets. In eight out of the ten interviews, the French nationals expressed that Europeans have easier times adapting to highly-regulated environments, another suggestion towards thoroughness-orientation. When discussing instances of sharing data, a majority of interviewees indicated more process-oriented tendencies. One interviewee from a French startup described data as “belonging to the end consumer”⁴³ and that these users have control over their information. This statement suggests more process-oriented ways of viewing data as the interviewee acknowledges the limits of French businesses’ ownership or rights to users’ data.

Amongst all the interviews stands out a discussion with one French technologist, Jena Selle. She posited that “French nationals [sic] tend to focus on three things: environment, economic

⁴¹ Interview by the author, Viva Technology Conference, Paris, France, May 17, 2019.

⁴² Interview by the author, Viva Technology Conference, Paris, France, May 18, 2019.

⁴³ Interview by the author, Viva Technology Conference, Paris, France, May 18, 2019.

protection, and human rights.”⁴⁴ Selle explains how French people do not support government efforts that infringe on these three basic rights and that quotidian market interactions are not sufficient for ensuring these rights. This assertion describes thoroughness and process tendencies and opens up to discussion about whether the cultural tendencies and history of actions by French nationals would seem to reflect these main points.

Relevant Histories Pointing to Current Biases

Compared to the United States, France as a nation has a long and rich history. This lengthy record gives reason to the appreciation of tradition and thus thoroughness-oriented cultural tendencies. There are cosmetic examples of this preference, such as the prevalence and preservation of Haussmann architecture throughout Paris. But other times tradition continues strong in areas on a government-scale like racial-blindness in the 21st century, which some believe is more harmful than helpful⁴⁵. Considering the interview with the French technologist, Jena Selle, there should be recurring instances in history where French society has expressed French citizens could be more sensitive to issues that could threaten the environment, the citizens’ economic protection, and the citizens’ human rights. A relevant example of the state’s human rights efforts is the French provisions to the GDPR through the 2004 Information Technology and Civil Liberties Act, which delineates consultation to the CNIL first before

⁴⁴ Jenna Selle, interview by the author, Viva Technology Conference, Paris, France, May 2019.

⁴⁵ Hargreaves, Alec G. 2015. “Empty Promises? Public Policy Against Racial and Ethnic Discrimination in France.” *French Politics, Culture & Society* 33 (3): 95–115. doi:10.3167/fpcs.2015.330305.

processing biometric data⁴⁶. But there are stronger examples throughout history from galvanized French citizens that demonstrate the society's value for human rights protections.

While the State exercises rights to pass protective legislation, from a societal standpoint, the French people have a history of mobilizing against institutions to protect their causes as well. My stay in Paris started at the 11th weekend of the "Gilets Jaunes" protests and lasted through the 29th weekend. Aside from that recurring protest, there still existed simultaneous smaller strikes or demonstrations from disgruntled French nationals for causes like transportation labor rights. There's an inherent acceptance of radicalism in France, which comes from a combination of political organization of French unions and French public policymakers. Of the last few decades, French unions were responsible for roughly half of the mobilized street protestors⁴⁷. Understandably, the French government is accepting or at least complicit to the unions as well by allowing their widespread presence through the French working economy. An environment that allows unions has stronger group-oriented cultural tendencies if the state desires to protect individuals from organizations, but at the same time existence of the unions themselves suggest stronger independent-oriented tendencies as the state is giving individuals opportunities or platforms to voice their grievances. This can also indicate network tendencies in workers' desires to build relationships through workers unions to protect their individual rights. These cultural tendencies have been rooted in French tradition. One interviewee's commentary on this

⁴⁶ Claire Gayrel, "The Principle of Proportionality Applied to Biometrics in France: Review of Ten Years of CNIL's Deliberations.," *Computer Law & Security Review*, <https://doi.org/10.1016/j.clsr.2016.01.013>.

⁴⁷ Marcos Ancelovici, "In Search of Lost Radicalism: The Hot Autumn of 2010 and the Transformation of Labor Contention in France," *French Politics, Culture & Society*, 127, <https://doi.org/10.3167/fpcs.2011.290308>.

environment is that “as a French person, the right to protest is one of our basic rights.”⁴⁸ It is clear that French society has ingrained the idea of group organization as a vehicle for the French to protect their individual liberties, irrespective of the exact cause.

⁴⁸ Interview by the author, Viva Technology Conference, Paris, France, April 29, 2019.

CHAPTER 5: CONCLUSIONS

From the VivaTech EU Commissioners’ panel there is one strong theme that seems to be a deciding factor in how the United States and France approach the topic of cyber policy: how each society defines innovation. In the case of the EU, and by extension France, innovation is all about inclusiveness and fairness. Whether that manifests itself in a fair approach to taxation or a data breach notification, there is strong belief that a pro-digital competitive economy should challenge inequality. From a study produced by RSA and exhibited in Figure 4, the level of comfort when it comes to data use and sharing varies by 15% between the US and France. When conversations surrounding data privacy had such strong thoroughness-oriented attitudes about the idea of fairness and minimization of inequality, it is more obvious to see how French nationals find that companies are not as likely to use data in an ethical manner. Whether that comes from natural skepticism or a belief that there aren’t currently procedures in place that guarantee an ethical use of data, French individuals hold more critical views of corporate holds on PII.

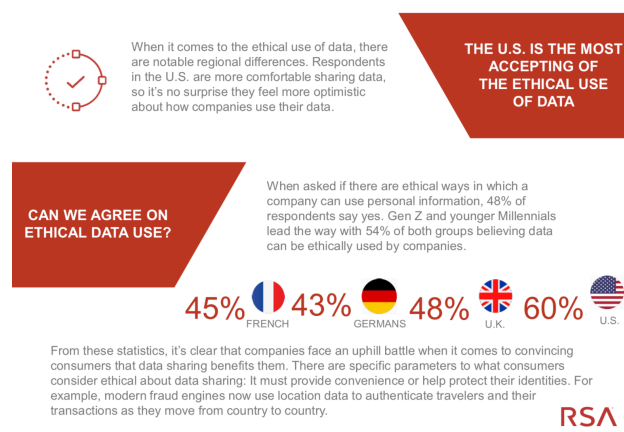


Fig. 4, RSA Data Privacy and Security Survey 2019: The Growing Data Disconnect between Consumers and Businesses, Page 11, September 2019.

Conversely, in the United States, the cultural tendencies that support the efforts and rights of an individual — in a more formal sense, the idea of a meritocracy, and in an informal sense the right to share information online — make an environment that supports the idea that innovation comes from individual, opportunistic efforts instead. Boasting 60% of belief that companies have the capability to use data in an ethical manner, the opportunity-oriented attitudes are clearly present in this situation. There are more cultural tendencies that seem to indicate that using data aids more to the innovation effort than withholding it. And in the realm of public policy, while there exists a number of laws that are in place to protect an individual's personal information, overall the United States has been late to recognize the digital economy as a environment in need of reform thanks in part to the strong network-oriented cultural tendencies that value the newer models of technological business. However, attitudes from US citizens concerning the invasiveness of company use of personal information suggests that there is potentially a shift in values for US society on the involvement dimension from a process-orientation to a network-orientation. Americans are becoming less optimistic on the control they have over their information. Attitudes in the cases of information collection to protect public and private interest are optimistic to a degree, but in general values that are in support of innovation are disjointed from how innovation typically happens.

The goal of this paper was not to point out whether or not the United States or France is better at handling the situation of cyber policy. Instead, the goal was to take a snapshot of both cases at this point in technological innovation and public policy and see how cultural attitudes are or are not influencing the current political landscapes for these two countries. From the analysis, we see

that tradition continues to be a deciding factor in how French individuals approach the topics of policy change, being less tolerant than Americans to change when it threatens certain individual liberties. For Americans, cultural tendencies have been strongly opportunity-oriented and value was mostly placed on the individual with the nuance of personal decision over an inherent personal freedom. But unlike France, Americans are perceiving a change in the digital economy that has not aligned with past experiences in public policy. Despite repeated cases for American public policy to be re-evaluated to be more reflective of the American people's distrust in the way organizations handle their personal data, the American people lack the environment to organize and protest like French citizens have the liberty of doing. Whether or not that is truly an effective means of invoking change in public policy is a discussion worth further evaluation, but this case would suggest that French ways of organization could be more in-tune with the current digital economy over the Americans' method of personal decision-making.

The purpose of evaluating cultural tendencies for technology and regulation is to understand to what degree societal values explain public policy. As we continue to observe innovations in the technology sector, it is important to consider the end users of these developments, whether French or American. With globalization increasing, it may no longer be possible to look to policies and values in one's country alone to survive in the digital economy.

Bibliography

Ancelovici, Marcos. "In Search of Lost Radicalism: The Hot Autumn of 2010 and the Transformation of Labor Contention in France." *French Politics, Culture & Society*. <https://doi.org/10.3167/fpcs.2011.290308>.

Auxier, Brooke, Lee Raine, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. November 15, 2019. <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

Bossi, Jeanne. "European Directive of October 24, 1995 and Protection of Medical Data: The Consequences of the French Law Governing Data Processing and Freedoms." *European Journal of Health Law* 9, no. 3. <https://doi.org/10.1163/157180902760498742>.

"Breach Notification." DLA Piper. Last modified January 23, 2019. Accessed October 18, 2019. <https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=FR>.
Overview of breach notifications in France.

Burden, Kit. "EU Update." *Computer Law & Security Review* 35, no. 1 (February 2019). <https://doi.org/10.1016/j.clsr.2018.12.007>.

———. "EU Update." *Computer Law & Security Review* 35, no. 4 (August 2019). <https://doi.org/10.1016/j.clsr.2019.06.005>.

Custers, Bart, Francien Dechesne, Alan M. Sears, Tommaso Tani, and Simone van der Hof. "A Comparison of Data Protection Legislation and Policies across the EU." *The Computer Law and Security Review* 34, no. 2. <https://doi.org/10.1016/j.clsr.2017.09.001>.

Cutler, Samantha. "The Face-Off between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information." *Boston College Law Review*. <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=129454710&site=ehost-live>.

"The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information." *Duke Law Journal*. Academic Search Complete (133418287).

Determann, Lothar. "Social Media Privacy: A Dozen Myths and Facts." Abstract. *Stanford Technology Law Review*, July 2012. <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=91596169&site=ehost-live>.

Epstein, Richard A. "Can Technological Innovation Survive Government Regulation?" *Harvard Journal of Law and Public Policy*.

"At bottom, the proper inquiry never poses the stark choice of regulation versus no regulation."

"European Commission." European Union. https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en.

Fazlioglu, Müge. "Beyond the 'Nature' of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States." *Fordham Urban Law Journal*. 46, no. 2 (April 2019). <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=136193122&site=ehost-live>.

Finney, Russ. Interview by the author. Online, Arlington, TX. April 10, 2020.

Gayrel, Claire. "The Principle of Proportionality Applied to Biometrics in France: Review of Ten Years of CNIL's Deliberations." *Computer Law & Security Review*, 450-61. <https://doi.org/10.1016/j.clsr.2016.01.013>.

Interview by the author. McCombs School of Business, Austin, TX. November 22, 2019.

Interview by the author. McCombs School of Business, Austin, TX. March 6, 2020.

Interview by Zoë Truong. Viva Technology Conference, Paris, France. May 18, 2019.

Kesan, Jay P., Carol M. Hayes, and Masooda N. Bashir. "A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy." *Indiana Law Journal* 91, no. 2 (Winter 2016). <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=113199291&site=ehost-live>.

Lebeau-Marianna, Denise. *Data Protection Laws of the World*. January 23, 2019. Accessed October 18, 2019. <https://www.dlapiperdataprotection.com/index.html?t=law&c=FR>.

McCall, Leslie, Derek Burk, Marie Laperrière, and Jennifer A. Richeson. "Exposure to Rising Inequality Shapes Americans' Opportunity Beliefs and Policy Support." *Proceedings of the National Academy of Sciences of the United States of America*. <https://doi.org/10.1073/pnas.1706253114>.

Mendez, Deirdre Brown. *The Culture Solution: How to Achieve Cultural Synergy and Get Results in the Global Workplace*. Boston, MA: Intercultural Press, 2017.

Nadeau, Richard, Vincent Arel-Bundock, and Jean-François Daoust. "Satisfaction with Democracy and the American Dream." *Journal of Politics*. <https://doi.org/10.1086/703070>.

Petersen, Kyle. "GDPR: What (and Why) You Need to Know about EU Data Protection Law." *Utah Bar Journal* 31, no. 4. <http://ezproxy.lib.utexas.edu/login?url=http://>

search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=130821070&site=ehost-live.

Pouillet, Yves. "Is the General Data Protection Regulation the Solution?" *Computer Law and Security Review*, 773-78. <https://doi.org/10.1016/j.clsr.2018.05.021>.

Problèmes Rencontrés. Illustration. CNIL. October 16, 2018. <https://www.cnil.fr/fr/violations-de-donnees-personnelles-1er-bilan-apres-lentree-en-application-du-rgpd>.

RSA Data Privacy and Security Survey 2019: The Growing Data Disconnect between Consumers and Businesses. September 2019. <https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf>.

Sanders, Amy Kristin. "The GDPR One Year Later: Protecting Privacy or Preventing Access to Information?" *Tulane Law Review* 93, no. 5 (May 2019). <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=137020794&site=ehost-live>.

Schechner, Sam. "Corporate News: France Turns Screw on Google Data Use." In *Factiva*. Previously published in *The Wall Street Journal*, September 28, 2013. <http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=90446174&site=ehost-live>.

Schröder-Ringe, Philipp. "The Amount of Data Breach Notifications in Germany and Europe Exploded since 25th May 2018." Härting. Last modified September 20, 2018. Accessed October 18, 2019. <https://www.haerting.de/neuigkeit/amount-data-breach-notifications-germany-and-europe-exploded-25th-may-2018>.

Selle, Jenna. Interview by Zoë Truong. Viva Technology Conference, Paris, France. May 2019.

Sullivan, Clare, and Sophie Stalla-Bourdillon. "Digital Identity and French Personality Rights – a Way Forward in Recognising and Protecting an Individual's Rights in His/Her Digital Identity." *Computer Law and Security Review*. <https://doi.org/10.1016/j.clsr.2015.01.002>.

Taylor, Laura. "Chapter 13 - Conducting a Privacy Impact Assessment." *ScienceDirect*. <https://doi.org/10.1016/B978-159749116-7/50018-4>.

"Violations de Données Personnelles : 1er Bilan Après L'entrée en Application du RGPD." Last modified October 16, 2018. Accessed October 18, 2019. <https://www.cnil.fr/fr/violations-de-donnees-personnelles-1er-bilan-apres-lentree-en-application-du-rgpd>.

CNIL published site on data breaches after GDPR

Wong, Rebecca. "The Data Protection Directive 95/46/EC: Idealisms and Realisms."

International Review of Law, Computers & Technology 26, no. 2/3. <https://doi.org/10.1080/13600869.2012.698453>.

Ybarra, Laura. "The E.U. Model as an Adoptable Approach for U.S. Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany, and the United States." *Loyola of Los Angeles International & Comparative Law Review*.
<http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=91026275&site=ehost-live>.

BIOGRAPHY

Zoë Truong was born in Dallas, Texas on September 11, 1997 and lived with her family in Arlington, Texas her entire life before college. In 2016, she enrolled in the Plan II Honors Program and the McCombs School of Business where she later majored in Management Information Systems after discovering a deep interest in the creative power of computer programming. Throughout college, she was actively involved in the Buddha's Light International Association - Austin Young Adult Division and a mentor for Code Orange. After UT, she will pursue a career in technology consulting with PricewaterhouseCoopers in Dallas.