CYBERSECURITY AND THE RIGHTS OF THE INTERNET USER IN FRANCE

Jennifer Cross[*]

TABLE OF CONTENTS

---

[*] Jennifer Cross is an alumni of the University of Georgia School of Law. She graduated in May of 2017. She is currently employed at the Augusta Judicial Circuit Law Office of the Public Defender in Augusta, Georgia.

I. INTRODUCTION

The rise of technology and its role in acts of terror, specifically the attacks in Paris on November 13, 2015, have reopened a longstanding debate on how state governments should regulate internet usage.[1] As accessibility to technology increases, a complicated question arises: what is the proper method for governments to legislate the balance between national security and personal freedom when it comes to the internet? The French government recently reacted to the killing of political cartoonists with a new law that regulates and collects data on French citizens.[2] This Note will analyze whether the *Loi Relative au Renseignement* (Law Concerning Intelligence) infringes on basic rights guaranteed in the European Union Charter of Fundamental Rights (ECFR), beyond what is permitted under the margin of appreciation doctrine, so as to violate France's requirements under the ECFR.

Part One of this Note will examine the creation, implementation, and potential consequences of the *Loi Relative au Renseignement*, providing context to better understand the content of this law and how it will affect the lives of people using the internet in France. Part Two will discuss the ECFR and its relevance to the controversy. The most applicable rights to this discussion are an individual's right to private and family life and the right to protection of personal data, found in Articles 7 and 8 of the ECFR.[3] As a member of the European Union, France is bound by the rules of the community and is subject to the rulings of the European Courts. Part Three will analyze how the European Court of Justice, the highest European Union court, should rule on the validity of this law based on the text of the Articles, jurisprudence, and legislative history of the ECFR. The European Charter of Fundamental Rights establishes all of the fundamental rights protected in the European Union. If the European Commission should decide to bring France to the European Court of Justice, this Note concludes that the court would likely hold that *Loi Relative au Renseignement* violates France's obligations to Articles 7 and 8 of the Charter.[4]

---

[1] Damian Paletta, *Paris Attack Reopens U.S. Privacy vs. Security Debate*, WALL ST. J., Nov. 16, 2015, http://blogs.wsj.com/washwire/2015/11/16/paris-attack-reopens-u-s-privacy-vs-security-debate/.

[2] *See* Szuskin & Kedrida, *The French Sweeping Intelligence Law Goes into Effect!*, LEXOLOGY, Aug. 4, 2015, http://www.lexology.com/library/detail.aspx?g=694bce7d-5692-48ab-aa50-4ce4f6eafabb.

[3] EU Charter of Fundamental Rights (ECFR) No. 2000/C of Dec. 18, 2000, arts. 7, 8, 2010 O.J. C 364 at 10.

[4] There are several avenues for potential litigants in regards to this law. One option is for the European Commission to make a claim against France in the European Court of Justice. Another option is for a member state of the European Union to bring a claim against France in the European Court of Justice. Further, any member or citizen of the European Union could

II. STATEMENT OF FACTS: HISTORY, MOTIVES, AND CONSEQUENCES

A. Motive Behind the Creation of the Loi Relative au Renseignement

On January 7, 2015, two members of Al-Qaeda entered the office of the satirical newspaper *Charlie Hebdo*, where they killed twelve people.[5] The newspaper was targeted because it had published cartoons of the Prophet Muhammad. The incident culminated in a shootout between the Al-Qaeda members and law enforcement. The event shocked the French public.[6] Three days later, approximately 4 million people in Paris participated in a rally of national unity.[7] Within two days, the Twitter hashtag *#jesuischarlie* had been tweeted over 5 million times.[8] The rally and social media attention the shooting received were seen not only as a way to support the victims' families, but also as a unified message from the French people in support of freedom of speech.

A few months later, in May 2015, a bill entered the French Parliament seeking to regulate and collect data in order to combat terrorism.[9] This bill was hotly contested by the French public, with some critics referring to it as the "French Patriot Act," a reference to the United States' Patriot Act that was passed in the wake of the 9/11 terrorist attacks.[10] These critics claimed the law would create a police state in France that would rival the government in George Orwell's *1984*.[11] Despite this criticism, by June 9, 2015, the French National Assembly and Senate passed the *Projet de Loi Relative au Renseignment* by an overwhelming majority.[12] The law allows the French government to monitor internet usage through complicated algorithms,

---

make a claim against France in the European Court of Human Rights. This paper will only analyze the first of these options.

[5] *Le Resume des Faits*, LE PARISIEN (Jan. 16, 2015), http://atelier.leparisien.fr/sites/Je-Suis-Charlie/les-faits/le-resume-des-faits.

[6] *Id*.

[7] Remi Piet, *Why Satire is Holy to the French*, AL JAZEERA (Jan. 14 2015), http://www.aljazeera.com/indepth/opinion/2015/01/why-satire-holy-french-islam-201511312482960735 0.html.

[8] *#JeSuisCharlie Tweeted More than 5 Million Times*, NEW DELHI TELEVISION LIMITED (Jan. 10, 2015), http://www.ndtv.com/world-news/jesuischarlie-tweeted-more-than-5-million-times-725090.

[9] *French Parliament Approves New Surveillance Rules*, BRITISH BROADCASTING CORPORATION (May 6, 2015), http://www.bbc.com/news/world-europe-32587377.

[10] *Lawmakers Back Spy Bill Dubbed 'French Patriot Act,'* FRANCE 24, (May 5, 2015), http://www.france24.com/en/20150505-lawmakers-back-spy-bill-dubbed-french-patriot-act.

[11] *Id. See also French Lower House Passes Sweeping Security Bill Some Call Patriot Act à la française*, FREE SPEECH RADIO NEWS (May 5, 2015), http://fsrn.org/2015/05/french-lower-house-passes-sweeping-security-bill-some-call-patriot-act-francaise/.

[12] *French Senate Passes Intelligence Bill*, WALL ST. J., June 9, 2015, http://www.wsj.com/articles/french-senate-passes-intelligence-bill-1433872098.

commonly referred to as *boites noires*, or "black boxes," based on an individual's internet usage.[13] This kind of technology is new and sophisticated, and therefore there is not a great deal of information available. Further, the details of the algorithm are classified, though internet service providers (ISPs) are required to use these algorithms and make the information readily available to French intelligence services.[14]

The law also allows the French government to monitor a person's web searches, e-mails, and mobile phone calls more intrusively than before, without requiring permission from a judge.[15] Some of the more intrusive measures include planting cameras, microphones, and recording keystroke logs.[16] The French Prime Minister bears ultimate responsibility for authorizing these measures. The Prime Minister is required to consult with a new, nine-person body, known as the National Committee of Intelligence Techniques Control, before engaging in these types of surveillance techniques; however, he does not have to follow the Committee's recommendations. The panel is made up of two deputies, two senators, two members of the Couseil d'Etat or State Council, two judges, and an electronic communications expert.[17]

B. Public Backlash

Hundreds of people attended protests in France leading up to the passage of this new law.[18] Protesters claimed that the proposed vast unchecked

---

[13] *Lawmakers Back Spy Bill Dubbed 'French Patriot Act*,*'* FRANCE 24 (May 5, 2015), http://www.france24.com/en/20150505-lawmakers-back-spy-bill-dubbed-french-patriot-act.

[14] *Id.* Another criticism of this law is that the French government is forcing ISPs to implement automatic data-processing software that will sort through data and requiring them to make the information acquired by the software readily available at all times. *See* Bertrand Liard & Alexis Tandeau, *New French Act on Intelligence Services: Impacts on Technical Operators*, WHITE & CASE TECHNOLOGY NEWSFLASH (Sept. 11, 2015), http://www.whitecase.com/publications/article/new-french-act-intelligence-services-impacts-technical-operators.

[15] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912, July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735.

[16] Angelique Chrisafis, *France Passes New Surveillance Law in Wake of Charlie Hebdo Attack*, THE GUARDIAN, May 5, 2015, http://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack.

[17] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912, July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA République Française [J.O.], July 26, 2015, p. 12735 art. 831-1. For more detailed information about the structure of the French parliament see FR. CONSTIT. Title IV arts. 24–33 (2008).

[18] *See French Privacy Advocates Protest New Spying Laws*, RUSSIA TODAY (Apr. 14, 2015), https://www.rt.com/news/249409-france-protest-spying-bill/.

powers posed a threat to their civil liberties.[19] Many human rights, internet rights, and civil rights groups joined the protests. One such advocacy group, *Quadrature du Net*, wrote, "Representatives of the French people have given the Prime Minister the power to undertake massive and limitless surveillance of the population . . . by doing so, they're ensuring the power of the state and the basis of our democratic system are getting ever more distant from one another."[20] Today, when so much of an individual's personal and business lives are online, this message resonated with millions of French people, despite the law receiving overwhelming support in the French parliament.

C. French Constitutional Court

The French Conseil Constitutionel, or Constitutional Court, is a body that decides whether a proposed law will go into effect. Cases can come to the Constitutional Court upon recommendation arranged by French officials, including: the President; the Prime Minister; the President of the National Assembly; the President of the Senate; a group of sixty members of the National Assembly; a group of sixty members of the Senate; or in special circumstances, other French courts.[21] If the Constitutional Court determines that a law violates the Constitution, the decision is binding and cannot be appealed.[22] Since the *Loi Relative au Renseigment* sparked so much controversy, President François Hollande submitted it to the Constitutional Court before it was implemented.[23] The Constitutional Court upheld the law on July 16, 2015, and it subsequently went into effect.[24] However, the Court did hold two aspects of the law unconstitutional: first, the provision allowing surveillance by French intelligence services abroad; and second, the provision allowing authorities to bypass the Prime Minister and the National Committee of Intelligence Techniques Control in "emergency" situations.[25] The Constitutional Court was concerned that what qualified as an "emergency" situation was not defined and could potentially result in

---

[19] *Id.*

[20] *L'Assemblée nationale vote la surveillance de masse des citoyens français*, LA QUADRATURE DU NET: INTERNET ET LIBERTÉS (May 5, 2015), https://www.laquadrature.net/fr/lassemblee-nationale-vote-la-surveillance-de-masse-des-citoyens-francais.

[21] 2008 FR. CONST. Title VII Art. 61.

[22] *Id.* art. 62.

[23] Emile Picy & Leigh Thomas, *French Constitutional Body Approves Eavesdropping Law*, REUTERS, July 23, 2015, http://www.reuters.com/article/us-france-surveillance-idUSKCN0PX2QF20150723.

[24] *Id.*

[25] Conseil constitutionnel [CC] [Constitutional Court] decision No. 2015-713 DC, July 23, 2015, J.O. 0171 (Fr.).

executive abuse. The French Constitutional Court upheld the rest of the law, including both the mass collection of metadata and the utilization of the law without the permission of a judge, even for the more serious surveillance measures. Unfortunately, the Constitutional Court was the last resort for French citizens to voice their concerns about the *Loi Relative au Renseignement* within France.

D. 13/11 Terrorist Attacks in Paris

On November 13, 2015, a terrorist group known as the Islamic State of Iraq and the Levant claimed responsibility for a series of deadly assaults in Paris that killed more than 100 people. Reports indicated that the massacre was the deadliest attack in France since World War II.[26] The assailants directed their violence against civilian populations at a concert hall, a soccer game, and several restaurants. After the fighting ended, France and the rest of the world were astonished at the carnage and grief-stricken with loss. In the following days, France launched a military bombing of the Islamic State's capital in Raqqa, Syria.[27] France also called for a military coalition to remove the group from power.[28]

France declared a state of emergency and also passed a law allowing that state of emergency to continue until February 2016.[29] This law expanded the July 2015 *Loi Relative au Renseignement*, by allowing police to conduct physical searches of electronic items like personal computers without warrants.[30] This law also allowed the government to conduct warrantless searches of homes and cars, strictly limit organized protests, and give the Prime Minister the power to immediately shutdown websites that are believed to pose a public security risk.[31] Due to subsequent attacks in

---

[26] Lori Hinnant & Greg Keller, *120 Dead in Paris Attacks, Worst Since WWII*, ASSOCIATED PRESS (Nov. 13, 2015), http://www.seattletimes.com/nationa-world/french-police-report-shoo tout-and-explosion-in-paris/.

[27] John Irish & Gregory Blachier, *'Spider in web' Mastermind of Paris Attacks Killed in Raid*, REUTERS (Nov. 19, 2015), http://www.reuters.com/article/2015/11/20/us-france-shooting –idUSKCN0T22IU20151120#RowwFGMWOd5FzDct.97.

[28] *Id*.

[29] Loi 55-385 du 3 avril 1995 de relative à l'état d'urgence et renforçant l'efficacité de ses dispositions [Law 2015-912 of July 24, 2015 relating to the state of emergency and reinforcing the effectiveness of its positions], http://www.assemblee-nationale.fr/14/projets/pl3225-ei.asp.

[30] *État d'urgence : l'État policier pour éluder tout bilan critique*, QUADRATURE DU NET: INTERNET & LIBERTÉS, Nov. 19, 2015, https://www.laquadrature.net/fr/etat-urgence-etat-polic ier.

[31] Loi 55-385 du 3 avril 1995, *supra* note 29.

France, the state of emergency has been extended until July 2017 after the next national elections.[32]

E. European Court of Justice

After the original intelligence law went into effect in July 2015, the political climate in Europe changed significantly. The November 2015 terrorist attacks in France further solidified fears that France is at risk of another attack. Despite the lack of relief in the national court system, there is still an avenue for individuals who believe that this law violates their civil rights. Since all national resources have been exhausted, it is possible for the European Commission to bring suit against the French government in the European Court of Justice.

The *Loi Relative au Renseignement* is being discussed by the Committee of Civil Liberties, Justice and Home Affairs of the European Parliament (the LIBE committee), after a request was made by members of the Alliance of Liberals and Democrats, a transnational centrist liberal political party, in the European Parliament.[33] The LIBE committee is a standing committee responsible for protecting the rights listed in the ECFR. Of additional concern is whether the European Union buildings located in Strasbourg, France, are subject to the July 2015 surveillance law, because if they are, then the law would subject other countries' sensitive information to French government surveillance.[34] After a thorough investigation has been completed, the LIBE committee will determine whether there is sufficient evidence to support a claim that France has failed to meet its European Union legal obligations as required under the ECFR. Many individuals have legitimate concerns about public security after the terrorist attacks in Paris, and if the LIBE committee chooses to bring a case against France for potential violations of their obligations under European Union law, the case could prove to be a historic opportunity for the court to show its commitment to the protection of fundamental rights.

---

[32] Nicolas Boring, *France: State of Emergency Extended to July 2017*, LIBRARY OF CONGRESS GLOBAL LEGAL MONITOR (Dec. 29, 2016), http://www.loc.gov/law/foreign-news/article/france-state-of-emergency-extended-to-july-2017/.

[33] *French Intelligence Law: European Commission Expresses "Serious Legal Concerns,"* DIPLOMATIC INTELLIGENCE (June 26, 2015), http://www.diplomaticintelligence.eu/european-union-news/765-french-intelligence-law-european-commission-expresses-serious-legal-concerns.

[34] *Id.* The Council of Europe and the European Parliament occupy buildings in Strasbourg. These buildings are international in nature, and collecting information through algorithms on world leaders in a space that is supposed to be reserved for diplomatic purposes may carry additional legal implications.

III. STATEMENT OF APPLICABLE LAW: FRENCH LAW AND EUROPEAN UNION LAW

A. Loi Relative au Renseignement

After the Constitutional Court upheld this legislation, the *Loi Relative au Renseignement* became law in France. Its goal is to ensure the security of France against future terrorist threats.[35] The law is designed to achieve this goal by using algorithms that allow the government to collect and analyze metadata through the internet. Information relating to the operation and implementation of the algorithm will likely remain unavailable to the general public.[36] The *Loi Relative au Renseignement* requires that ISPs allow the government to implement these algorithms on their networks and make the information collected available to the government. The law specifically says, "for the sole purpose of preventing terrorism, it may be imposed on operators' . . . automated processing networks, according to the parameters specified in the authorization, to detect likely connections that can reveal a terrorist threat."[37] A provision of the law also permits the government to use the algorithm to collect metadata that contains confidential information of lawyers, journalists, judges, and members of the legislature.[38] This means that all French internet users are subject to government surveillance even without any evidence of wrongdoing on their parts.

The law also requires that a nine-person panel, the National Committee of Intelligence Techniques Control, will be used to determine whether, based on the results of the algorithm, a subject of surveillance may be subjected to still more intrusive investigation.[39] The *Loi Relative au Renseignement* states that members of this oversight board have specified term limits, and it is designed to ensure equal representation of men and women.[40] Further, the law puts into place a system of communication between the National Committee of Intelligence Techniques Control and the Prime Minister.[41] The oversight

---

[35] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912 of July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735 art. 811-2.

[36] Assemblée Nationale- 2e Séance du 2015, JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], April 15, 2015, p. 4200.

[37] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912, July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735 art. 851-3.

[38] *Id.* art. 821-7.

[39] *Id.* art. 831-1. For more detailed information about the structure of the French parliament see 2008 FR. CONST. Title IV art. 24-33.

[40] Loi 2015-912 du 24 juillet 2015, *supra* note 37, art. 831-1.

[41] *Id.* art. 833-4–833-11.

board is meant to act as a check on the Prime Minister's power, but some find that it lacks effective democratic and judiciary mechanisms. For example, French anti-terrorist judge Marc Trevidic stated, "These exorbitant powers will be without judicial review. Do not lie to [the] French by presenting this project as an anti-terrorism law. It opens the way to widespread intrusive methods, beyond the control of court judges, guarantors of individual freedoms in our country."[42] The National Committee of Intelligence Techniques Control's lack of authority to stop the Prime Minister's decision to conduct more aggressive surveillance measures may present another legal issue with regard to France's European Union obligations.

B. European Court of Justice

If the European Commission chooses to assert a claim against France in the European Court of Justice, the court will look to several sources of law, jurisprudence, and legal writings in making its final determination. The court will likely look to Articles 7 and 8 of the ECFR, the legislative history behind these Articles, and previous rulings by various European Union courts, such as the European Court of Human Rights.

The *Treaty Establishing the European Steel Community* (now known as the *Treaty of Paris 1951*) brought about the creation of the European Court of Justice in 1952.[43] The mission of the court is to interpret how the law should be followed and to ensure the law is observed equally among its treaty members.[44] This court is the most powerful in the European Union, and it has the last word on the interpretation of European Union laws.[45]

Since 1951, the role of the court has expanded as the European Union has grown. The most notable of these expansions was achieved through *Flamingo Costa v. ENEL*, wherein the European Court of Justice established the supremacy of European Union law over that of its member states.[46] This allows the court to make rulings that are binding on member states, including

---

[42] Eric Palletier, *Projet de loi sur le renseignement: les réserves du juge antiterroriste Marc Trévidic*, L'EXPRESS, Mar. 19, 2015, ["Ces pouvoirs exorbitants se feront sans contrôle judiciaire. Ne mentons pas aux Français en présentant ce projet comme une loi antiterroriste. Il ouvre la voie à la généralisation de méthodes intrusives, hors du contrôle des juges judiciaires, pourtant garants des libertés individuelles dans notre pays"], http://www.lexpress.fr/actualite/projet-de-loi-sur-le-renseignement-les-reserves-du-juge-antiterroriste-marc-trevidic_1662838.html.

[43] Treaty Establishing the European Steel Community, Arts. 31–48, Apr. 15, 1951, 261 U.N.T.S. 140.

[44] *Id.* art. 31.

[45] *Id.*

[46] 594 Case 6/64, Flamingo Costa v. Enel, 1964 E.C.R. 585.

France, and to ensure compliance with European Union laws and treaties. Another significant European Union Court of Justice case was *Van Gend en Loos v. Nederlandse Administratie der Belastingen*.[47] In this case, the European Court of Justice held that the European Community can create rights for European Union citizens that can be enforced by member countries' national courts.[48] These rulings have made the court relevant in the member state's national legal systems and are designed to create a more uniform system of governance among the European states.

Since the European Court of Justice is considered to be the highest court, it can only hear cases if certain conditions are met. First, the law of the member state must be in conflict with European Union law, and every other national avenue must be exhausted.[49] Second, there are two types of claimants who can bring a suit to the European Court of Justice. One is the European Commission.[50] The members of European Commission are referred to as the "guardians of the treaty," and they are responsible for monitoring member states to ensure compliance with the treaties of the European Union.[51] The other is another member state could bring a claim against a country it alleges has violated European Union law. This does not happen as often, however, due to potentially adverse political consequences.[52]

C. European Union Charter of Fundamental Rights

The treaty that is the main focus of this Note is the European Charter of Fundamental Rights (ECFR). As the European Union grew in membership, one major issue the community faced was how best to consolidate the member states' legal systems into a harmonized regime, within which certain personal, political, civic, economic, and social rights were protected.[53] The system previously in place was especially confusing for E.U. citizens, because there was no uniformity among members, and people were unsure of their rights. Consequently, member states created the ECFR in 2000, to

---

[47] Case 26/62, Van Gend en Loos v. Nederlandse Administratie der Belastingen, 1963 E.C.R. 16.

[48] *Id.*

[49] Vaughne Miller, *Taking a Complaint to the Court of Justice of the European Union, Library House of Commons (UK) SN/IA/5397* (Mar. 11, 2010), http://researchbriefings.Parliament.uk/ResearchBriefing/Summary/SN05397#fullreport.

[50] ALAIN A. LEVASSEUR ET AL., THE LAW OF THE EUROPEAN UNION 210, 452–57 (Carolina Academic Press 2d ed. 2013).

[51] Treaty of the European Union (Consolidated Version 2012) art. 17, Dec. 13, 2007, 298 U.N.T.S. 3, 2012 O.J. (C 326).

[52] LEVASSEUR ET AL., *supra* note 50, at 452.

[53] *Id.*

delineate these rights more clearly.[54] The ECFR has components that resemble a constitution, including a bill of rights and general principles for the European Union as a political entity.[55]

A typical problem in a two-tiered style of government is balancing the division of power. This stereotype held true for the European Union after the drafting of the ECFR. Some European states expressed concern that the power of the European Union was encroaching on national rights. After years of debate, the ECFR became binding in 2009, when the European Union adopted Article 6 of the Treaty of the European Union.[56] This treaty states, "the provisions of this Charter are addressed to institutions, bodies and organs of the Union with due regard for the principle of subsidiary and to the member states only when they are implementing Union law."[57] In other words, a violation of the ECFR can only be invoked when a member state is applying E.U. law or derogating from it.[58] Article 6 also gave the ECFR the same legal force as a treaty.[59]

The articles of the ECFR that are most relevant to the analysis of *Loi Relative au Renseignment* are Articles 7 and 8. When the European Court of Justice is determinating the legality of the *Loi Relative au Renseignement*, it will likely look to the text of these articles along with other secondary authorities to aid in its interpretation of the law.[60] In fact, the European Court of Justice held, in its 1974 judgment in *Nold v. Commission of the European Communities*, that it is "bound to draw inspiration from constitutional traditions common to the Member States," and that, "international treaties for the protection of human rights, on which the member states have collaborated or of which they are signatories, can supply guidelines which should be followed within the framework of community law."[61] This language leaves a lot of potential for the use of persuasive authority that is often absent in other legal systems.

---

[54] GIACOMO DI FEDERICO, THE EU CHARTER OF FUNDAMENTAL RIGHTS: FROM DECLARATION TO BINDING INSTRUMENT 7 (Springer 2011).

[55] *Id.*

[56] Treaty of the European Union (Consolidated Version 2012) art. 6, Dec. 13, 2007, 298 U.N.T.S. 3, 2012 O.J. (C 326).

[57] *Id.* art. 51.

[58] Case C-617/10, Åklagaren v. Hans Åkerberg Fransson, 2003 E.C.R. 340.

[59] *Id.*

[60] Some of the secondary sources the European Court of Justice has used in the past include the Commentaries of the ECFR, European Court of Human Rights decisions, and European Parliament Directives. It is noted that the Commentaries of the ECFR and European Court of Human Rights decisions have only persuasive value.

[61] Case 4/73, J. Nold, Kohlen- und Baustoffgroßhandlung v. Commission of the European Communities, 1974 E.C.R. 00491 at 507.

1. Article 7 Analysis

Article 7 requires European Union members to respect an individual's private and family life. Specifically, Article 7 of the ECFR states that, "everyone has the right to respect for his or her private and family life, home, and communications."[62] This is particularly applicable in the context of the *Loi Relative au Renseignment*, which allows the government to monitor the activities of all French internet users. This Article was written to protect individuals from expansive government intrusion.

In 2003, the European Parliament created the European Union Network of Independent Experts on Fundamental Rights (NIEFR).[63] This organization created a commentary that analyzes each article of the ECFR. This commentary spends some time discussing the significance of the word "communication" as used in Article 7. This word is of particular importance, because in contrast to other human rights treaties that use more narrow language, the creators of the Charter use the word "communication" broadly, with the intent to adapt to changes in technology.[64] Also, in comparison to other laws used in directives or other articles of this document, Article 7 uses expansive language, indicative of an expansive interpretation of this right.

The European Court of Justice may also look to previous case law in its analysis of Article 7, including that of the European Court of Human Rights, which acts as persuasive authority for these purposes. The European Court of Human Rights is a court established by the European Convention on Human Rights, and it rules on alleged violations of that Convention. The European Court of Justice looks to the European Court of Human Rights partially because it often looks to similar questions of civil, political, social, and economic rights. The European Court of Human Rights can only hear claims brought under the 1950 European Convention of Human Rights.[65] Since the adoption of the ECFR, however, the European Court of Justice has

---

[62] EU Charter of Fundamental Rights (ECFR) No. 2000/C of December 18, 2000, art. 7, 2010 O.J. (C 364) 10.

[63] European Parliament Resolution on the Situation as Regards to Fundamental Rights in the European Union, Parl. Eur. Doc. (COM 0606) 8 (2003).

[64] E.U. Network of Independent Experts on Fundamental Rights, Commentary of the Charter of Fundamental Rights of the European Union, at 78 (2000), http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf.

[65] European Convention of Human Rights, art. 19 (June 1, 2010), http://www.echr.coe.int/Documents/Convention_ENG.pdf.

frequently addressed human rights issues similar to those expressed in the European Convention on Human Rights.[66]

Much of the case law suggests that the European Court of Human Rights has broadly interpreted the right to respect for private and family life. For example, in *Lopez Ostra v. Spain*, the plaintiff asserted that her privacy rights were being violated because a government waste treatment plant was built only a few meters from her home, which greatly diminished her quality of life.[67] In its 1994 judgment in the case, the European Court of Human Rights ruled that severe environmental pollution, such as that caused by a waste treatment plant, could have secondary effects which could inhibit a person's right to private life.[68] Therefore, an individual's privacy rights could be violated, even through indirect means, if the government action was to interfere with his or her personal life choices.

Another European Court of Human Rights case that presented a similar question was *Klass v. Germany*.[69] The case involved the German government's interception of phone conversations and inspections of mail, which it said were intended to protect German democratic society from threats to national security and other crimes. In its 1978 decision, the European Court of Human Rights held it is sometimes necessary to conduct investigations of individuals secretly; however, in order to determine if a law violates an individual's privacy rights the court must analyze, "the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law."[70] The court eventually held that the German law did not constitute a violation, reasoning that, first, there was a strict time limit for the collection and retention of personal information, and second, the cases were subject to judicial review.[71]

These judgments show that although an individual's right to privacy is designed to be interpreted expansively, there is latitude for member states to maneuver. The jurisprudence also highlights the importance of communication between a government and its citizens. These cases indicate data collection is not necessarily an evil, so long as, first, the state clearly

---

[66] Elena Both, *The Roles and Relationship between the Two European Courts in Post-Lisbon EU Human Rights Protection*, JURIST (Sept. 12, 2013), http://jurist.org/dateline/2013/09/elena-butti-lisbon-treaty.php.

[67] Lopez Ostra v. Spain, App. No. 16798/90, Eur. Ct. H.R. 5 (1994).

[68] *Id.*

[69] Klass v. Germany, App No. 5029/71, 71 Eur. Ct. H.R. (ser. A.) at 18-19 (1978).

[70] *Id.*

[71] *Id.* at 9.

communicates how the data will be used, and second, the state provides a proper independent mechanism for review.

The European Court of Justice could also look to Article 17 of the International Covenant on Civil and Political Rights for guidance, because France is a party to this treaty.[72] Article 17 says, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[73] In other words, a government cannot indiscriminately interfere with individuals' private lives. The 2008 General Comments, accepted by the Human Rights Committee, say that for a government provision to not be arbitrary or unlawful, the law must be legal, meaning it does insofar as to not violate other international law provisions, was created to further the goals of the Covenant, and is reasonable under the circumstances.[74] The comments further state that the law must state in detail exactly when and how the interferences will be permitted.[75] Due to the similarity in phrasing between Article 17 of the International Covenant on Civil and Political Rights and Article 7 of the ECFR, Article 17 may provide a useful aid in understanding an individual's right to privacy.[76]

From the cases, treaties, and commentaries, there is a general consensus on what factors the court will likely use in determining whether the *Loi Relative au Renseignement* violates Article 7 of the ECFR. These factors will likely include the duration for which an individual is placed under surveillance, the period of time for which the information taken from that surveillance will be stored, the scope of the surveillance, and the overall reasonableness of the member state's legislation. The disputed area the court will have to define is where states draw the line between personal freedom and national security.

---

[72] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 177.

[73] *Id*.

[74] U.N. Hum. Rts. Committee, Gen. Comment No. 16, Art, 17, *Right to Privacy* (Sept. 28, 1988), http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en.

[75] *Id*.

[76] So far, the Human Rights Committee of the International Covenant on Civil and Political Rights have indicated in their state report that France's new surveillance law is in conflict with Article 17 of the International Covenant of Civil and Political Rights. *See* U.N. Human Rights Committee, *Pacte International Relatif aux Droits Civils et Politiques: Observations finales concernent le cinquième rapport périodique de la France*, art. 12 (Aug. 17, 2015), http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2ffFRA%2fCO%2f5&Lang=en.

2. Article 8 Analysis

The court may also find the *Loi Relative au Renseignement* violates Article 8 of the ECFR. Article 8 states the following:

> Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.[77]

This Article was specifically created to modernize privacy rights by protecting individuals from intrusive government monitoring. In order to more fully grasp this Article, the European Court of Justice will likely look at the text of the Article itself, the commentaries, European Union Parliament's legislation on this Article, and various case law.

NIEFR issued another comment in 2002 in response to the World Trade Center attacks on September 11, 2001. This commentary examines the balance needed in order to safeguard civil liberties guaranteed by the ECFR while also protecting individuals from terrorist threats.[78] In this comment, the organization focused heavily on the criteria necessary to retain an individual's personal information in light of the rights guaranteed to a person by the ECFR. Specifically, the data retention needs to be: for a specified time, for justified grounds, and monitored by an independent control authority in order to preserve the democratic integrity of the European Union.[79]

Another interpretative aid the court will likely use is European Union Parliament legislation. The European Parliament passed Directive 95/46/EC with the purpose of protecting European Union citizens with respect to the processing and collecting of personal data.[80] Since this directive was passed

---

[77] EU Charter of Fundamental Rights (ECFR) No. 2000/C of Dec.18, 2000, art. 8, 2010 O.J. (C 364) at 10.

[78] E.U. Network of Independent Experts on Fundamental Rights, *The Balance between Freedom and Security in the Response by the European Union and Its Member States to Terrorist Threats*, 7 (2002), http://ec.europa.eu/justice/fundamentalrights/files/cfr_cdf_themcomment1_en.pdf.

[79] *Id*. at 25.

[80] Directive 95/46/EC, of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31-50.

in 1995, there has been discussion in the European Union about updating the directive because of technological advances.[81] The directive says a government needs to meet seven criteria in order to collect an individual's personal data: first, it must provide notice that it is collecting an individual's personal data; second, the collection must be for a legitimate purpose; third, the subject of the data collection must give their consent; fourth, the data collected must be secure; fifth, the subject of the data collection must know who has his or her information; sixth, the subject of the data collection must have access to their data; and seventh, any organizations violating these principles must be held accountable.[82] The directive also defines the term "personal data" broadly, so as to afford more expansive rights. It describes personal data as any information that can be reasonably linked to a particular individual.[83] But this directive includes exceptions in order to combat potential threats to European Union security. Some of these exceptions include: national security, defense, public security, prosecution of criminal offenses, and certain economic interests of the state.[84] The competing interests between civil liberties and public security since then have been treated like a balancing test weighed by European courts like the European Court of Human Rights and the European Court of Justice. Although this directive lays out factors for courts to consider, its exceptions require the court to determine the validity of national laws on a case-by-case basis, which can often leave room for confusion among member states.

The European Court of Human Rights addressed the issue of personal data collection in 2000 in *Rotaru v. Romania*. There, a Romanian citizen brought a claim arguing that Romania's collection and use of his personal data was a violation of Article 8 of the European Convention on Human Rights.[85] Some of the personal data at issue in this case included the applicant's political writings before the collapse of Romania's Stalinist government, and incorrect information which affiliated him with a violent political group known as the Legionaries.[86] Article 8 of the European Convention of Human Rights, similar to Articles 7 and 8 of the ECFR, indicates that everyone has a right to private life.[87]

---

[81] 2013 Report on the Application of the European Union Charter of Fundamental Rights, at 46 (2013), http://ec.europa.eu/justice/fundamentalrights/files/2013_charter_report_full_version_en.pdf.

[82] Parliament and Council Directive 95/46, art. 7-10, 1995 O.J. (L 281).

[83] *Id*.

[84] *Id*. art. 13.

[85] Rotaru v. Romania, 8 B.H.R.C. 449 (2000).

[86] *Id*.

[87] European Convention on Human Rights, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

In its 2000 judgment, the European Court of Human Rights held the Romanian law violated Article 8 because the "domestic law was not sufficiently precise to indicate to citizens in what circumstances and on what terms the public authorities were empowered to file information on their private life and make use of it."[88] The court also held that the domestic law was not specific enough in how the government will use its data collection power, and there were not any safeguards against the potential abuse of this power.[89]

The Council of Europe indicated in both the ECFR and the European Convention on Human Rights that widespread and unchecked surveillance can become a governmental tool for oppression. Considering Europe's history of communism and fascism in the early twentieth century, this concern is legitimate. The judgment in *Rotaru v. Romania* indicated that in order to make a data-collection law legal, the state must include certain precautions to ensure the rights of European Union citizens are protected. One of these precautions is a clear message of what information is being collected and how it will be used by the member state's government. Failing to meet these requirements would be unjust, because it would render the data collection process completely arbitrary. This could potentially result in a state where everyone is subject to punishment for political, economic, or cultural views.[90] Further, the court emphasized the value of proper safeguards to ensure the purpose declared in the state law is being followed.[91] Without proper checks on government authority, there is little assurance that the data collection is being used legitimately.

The court will also likely look to *Digital Rights Ireland Ltd. v. Minister of Communications*.[92] In this European Court of Justice 2004 action, the Irish High Court and the Austrian Constitutional Court asked for a preliminary ruling on Directive 2006/24 created by the European Parliament. Directive 2006/24 was created in the wake of the terrorist attacks of September 11, 2001, in the United States. The directive allowed governments to collect data on an unlimited number of people and to store that data for an extended period of time, with the stated purpose of combating the threat posed by global terrorism.[93] The European Court of Justice found that the directive interfered with the European Union citizen's right to protection of their personal data

---

[88] Rotaru v. Romania, 8 B.H.R.C. 449 (2000).
[89] *Id.*
[90] *Id*.
[91] *Id*.
[92] Case C-293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Celex No. 612CJ0293, European Court Reports (Apr. 8, 2014).
[93] *Id*.

under Article 8 of the ECFR.[94] It also analyzed whether this directive met a public security exception. As mentioned previously, if a state is implementing a data-collection policy designed to counter crimes like terrorism, there is more flexibility in the ECFR. The court found the law in question did meet an exception, because the directive protected a legitimate interest: an individual's right to security, which is also protected by the ECFR.[95]

The next issue the court analyzed in its judgment in *Digital Rights Ireland* was whether the law was a proportional response to the security interest in light of Articles 7 and 8 of the ECFR. In this part of the opinion, the court analyzed to what degree the law was an acceptable way to achieve its purpose and whether the methods it implemented were necessary. The court wrote that considering the seriousness of the violation of Articles 7 and 8 of the Charter, the standard should be strict.[96] The court held that the generalized surveillance measures allowed in this directive were not necessary, because the surveillance measures did not require a link between the criminal activity that they were monitoring and the subject of the surveillance.[97] This generalized governmental surveillance could not be allowed because it essentially put everyone in the European Union under the microscope of the government. Further, the court held, there were improper safety mechanisms in place to ensure the data would be used for a legitimate purpose.[98]

This case indicates that member states have the ability to create policies to protect their vital security interests, but that those interests must be weighed against the fundamental rights and freedoms protected by the ECFR. Some elements to consider in this test are the seriousness of the threat posed, on the one hand, and the extent to which individual freedoms will be compromised, on the other. The judgment in *Digital Rights Ireland*, in particular, suggests the number of individuals being surveilled by the government is important in determining whether the data collection is unfair and arbitrary. Thus, when there are more people placed under surveillance there must also be a greater security interest.

3. Margin of Appreciation Analysis

The margin of appreciation doctrine allows states to have room to maneuver when it comes to developing state policy in order to implement European Union laws. Specifically, the Council of Europe stated in an

---

[94] *Id*.
[95] *Id*.
[96] *Id*.
[97] *Id*.
[98] *Id*.

Explanatory Report on Protocol that, "State Parties enjoy a margin of appreciation in how they apply and implement the Convention, depending on the circumstances of the case and the rights and freedoms engaged."[99] This doctrine was originally used in the European Court of Human Rights, but the European Court of Justice has also since adopted it.[100] There is often conflict when a two-tiered system is implemented between the state governments and the federation of states as a whole. In the case of the European Union, a source of tension between the community and the member states is that the community wants to develop a more uniform system of laws and regulations while states want to retain their sovereignty. The margin of appreciation doctrine offers a potential solution to this problem.

Some areas of the law allow more flexibility than others. These include public emergency, national security, protection of public morals, and legislative implementation of social and economic policies.[101] States also have more leeway when there is no universal consensus within the European Union, or if a state is trying to balance two competing rights.[102] The margin of appreciation doctrine is more open to these kinds of policies because certain regulations are sometimes necessary for security reasons that ensure the survival of the state. Also, states might be better qualified to make certain kinds of legislation because they are in "direct, continuous contact with the realities of the country" and can more accurately strike a balance between social needs.[103] When the European Court of Justice has to make rulings on whether or not a state policy violates European Union law it will likely analyze whether it fits into one of these categories.

Other kinds of state laws have a narrower margin of appreciation. Examples include when a person's identity or existence is at stake, a person's absolute rights are compromised, a law promotes racial or ethnic discrimination, or a law seeks to regulate an "intimate aspect of private life."[104] In these cases, the European courts are much less flexible because

---

[99] Council of Europe, *Explanatory Report on Protocol No. 15*, para. 9, http://www.echr.coe.int/Documents/Protocol_15_explanatory_report_ENG.pdf.

[100] C-83/94, Criminal Proceedings against Peter Leifer, Reinhold Otto Krauskopf and Otto Holzer 1995 E.C.R. I-3236.

[101] LUKASZ GRUSZCZYNSKI & WOUTER WERNER, DEFERENCE IN INTERNATIONAL COURTS AND TRIBUNALS: STANDARD OF REVIEW AND MARGIN OF APPRECIATION 240–42 (Oxford University Press 1st ed. 2014). The convention here refers to the European Convention on Human Rights which is used and interpreted by the European Court of Human Rights. The European Court of Justice has adopted a similar stance on the margin of appreciation doctrine and shows special presidential value to European Court of Human Rights cases.

[102] *Id.*

[103] Tammer v. Estonia, 2001-1 Eur. Ct. H.R. 27.

[104] *Id*.

there is a strong interest in promoting policy that guarantees the greatest amount of personal freedom and that protects individuals from those in power who may want to take advantage of political, ethnic, and racial minorities. The analysis becomes more complicated, however, when there are two fundamental rights directly at odds with each other.

IV. DISCUSSION: EUROPEAN COURT OF JUSTICE INQUIRY

This Note will next discuss how the European Court of Justice might rule if the *Loi Relative au Renseignement* was brought before it, considering the jurisprudence and the facts of this particular case. The first part of this section will analyze whether the *Loi Relative au Renseignement* violates Article 7 of the ECFR. The second part will discuss whether or not it violates Article 8. After looking at the facts of the case and the applicable law, the European Court of Justice will probably find this law violates Articles 7 and 8 of the ECFR. So, the third part of the discussion will try to determine if the law meets any of the enumerated exceptions in Articles 7 and 8. Finally, the fourth part will analyze whether the margin of appreciation doctrine provides enough latitude for the French government to keep their law even though it conflicts with the European Union obligations.

A. Does the French Law Violate Article 7?

Article 7 indicates that every individual has a right to private life. This right to not be interfered with has been the subject of a great deal of litigation and analysis.[105] If the European Commission were to bring a claim against France in the European Court of Justice, the Commission would likely claim that France had violated its obligations to be in compliance with the ECFR under Article 7. France would probably argue that this law is specific enough and has adequate safeguards to avoid violation. When determining whether the *Loi Relative au Renseignement* encroaches upon an individual's right to private life, special consideration must be given to the jurisprudence.

1. Arbitrary use of Surveillance

If the European Commission chooses to bring a suit against France to the European Court of Justice, the Commission will claim the *Loi Relative au Renseignement* violates Article 7 in several ways. One of these is that

---

[105] EU Charter of Fundamental Rights (ECFR) No. 2000/C of December 18, 2000, art. 7, 2010 O.J. C 364 at 10.

running all metadata used by French citizens through algorithms without discrimination is an interference with private life because personal information is being collected arbitrarily. The Commission will contend that screening the entirety of the French population to search for a fraction of the minority of persons who may attack the state is unfair in that it will force the rest of internet users to be subject to expansive police powers. Although certain qualifications must be met to further analyze the collected metadata, the collection of such information in the first place is an interference with the French population's privacy rights, and there is no way to check the power of French intelligence agencies.

The French government could argue this law does impose certain limits on the collected data. It might also assert that the collection of metadata alone should not be considered an interference with a person's fundamental rights, because simply holding the information for a specific period of time does not prevent the subject of the surveillance from accessing the information. Nor does the law allow intelligence services to use the data. Further, France will probably say that the complex algorithms do initially screen all of the data, but this information is not used unless certain qualifications are met. So, the search for information relating to a potential terrorist threat is not arbitrary.

In *Klass v. Germany* the European Court of Human Rights held the German government could collect data of a German citizen because there was a judicial measure in place that checked the power of intelligence agencies.[106] France will probably say in the case of the *Loi Relative au Renseignement*, all metadata is put through an algorithm without judicial discretion or control, but there are checks on more invasive measures of data collection because the National Committee of Intelligence Techniques Control reviews cases and gives a recommendation on an individual basis.[107] Further, the Prime Minister acts as a final check because he makes the final decision as to whether more invasive measures will be implemented.[108]

The European Court of Justice will probably find that the widespread collection of metadata for the purpose of putting it through an algorithm conflicts with an individual's right to a private life. Metadata alone may not necessarily give a lay-person enough data to link the information to an individual, but the information in metadata can be easily processed by an intelligence agency in order to reveal personal data that links directly to an

---

[106] Klass v. Germany, App No. 5029/71, 71 Eu. Ct. H.R. 214 (ser. A.).

[107] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912 of July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735.

[108] *Id.*

individual.[109] Since the information is being collected from all internet users in France and not only individuals who are suspected of committing criminal offenses, it seems to be an over inclusive policy that is only going to capture a small segment of the population while jeopardizing most people's individual liberties.

2. Lack of Governmental Transparency

The European Commission also might claim that there is no limit to how much information is being collected on an individual subject of surveillance. This results in uncertainty among internet users, and necessarily interferes with their private lives. Since only specific members of French intelligence agencies know how the algorithm works or what makes a French internet user subject to more intrusive measures of surveillance, the *Loi Relative au Renseignement* could discourage people from making statements that could be interpreted as against the French government. This kind of unregulated authority could end in a violation of a person's privacy rights, especially if a person may be subject to government monitoring for comments made in the private sphere.

The government might reply to this claim by saying that the algorithms used to screen the metadata are advanced and complex, and are designed to determine whether a surveillance subject's internet usage indicates that he or she would be a terrorist threat.[110] So, the fear that French intelligence services will use this power to quash political dissidents is not valid.

This question will be particularly difficult for the European Court of Justice because the issue of whether an algorithm that detects signs of terrorist sentiment is a sufficient measure of security has never been presented to the European Court of Justice or the European Court of Human Rights before. The European Court of Justice, in its 2014 judgment in *Digital Rights Ireland Ltd. v. Minister of Communications*, did hold that widespread surveillance of a population without checks on government power violates the individual's right to privacy.[111] But, the European Court of Human Rights in its 1978 judgment *Klass and Others v. Germany* determined that in other instances a government

---

[109] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ (L 281), 23.11.1995, p. 31.

[110] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912 of July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735.

[111] Cases C-932 & C-594 Digital Rights Ireland Ltd. and Kärntner Landesregierung, 2014 E.C.R. 238.

can collect more intimate data if there is just cause and proper evidence to support a more detailed investigation.[112]

Despite the arguments on both sides, the European Court of Justice will most likely find that these algorithms are not an appropriate measure to protect individuals from government intrusion into the privacy rights guaranteed by the ECFR. One of the main issues the European Court of Justice will have is that no one with actual independent authority can control the actions of the Prime Minister.[113] The French government could actually be screening for anything, and there is no governmental check on the intelligence agencies who are collecting data. Some of the information analyzed could be completely irrelevant to the prevention of terrorism.

Another reason why the European Court of Justice may find these algorithms to be an ineffective protection is because the algorithm, which is designed to act as a screen, does not actually protect an individual until after their metadata has already been collected and analyzed. One could argue there is an inherent violation of an individual's right to privacy, however, simply from the mere collection and storage of the data.[114]

3. Adequate Safeguards

The Commission should argue that the security measures that have been implemented to prevent the abuse of this authority are too few and lack transparency. Unlike surveillance laws in other countries, which require permission from a judge before engaging in what are arguably more intrusive surveillance practices, this law requires only the permission of the Prime Minister.[115] Further, although there are two judges on the National Committee of Intelligence Techniques Control, their opinions are neither binding nor enforceable and do not provide an effective check on the Prime Minister's authority.

The French government could reply by saying the Constitutional Court has already taken these concerns into account and has required the Prime Minister to seek the opinion of the National Committee of Intelligence Techniques Control before making a determination about engaging in more serious

---

[112] Klass v. Germany, App No. 5029/71, 71 Eu. Ct. H.R. (ser. A.).

[113] *France: Halt Rush Towards Surveillance State*, AMNESTY INTERNATIONAL (May 4, 2015), https://www.amnesty.org/en/latest/news/2015/05/france-surveillance-state/.

[114] Leander v. Sweden, 3 Eur. Ct. H.R. (ser. A) at 153 (1987).

[115] Nathan A. Sales, *French Surveillance Law Compared to U.S. Surveillance Law* (July 31, 2015), http://insct.syr.edu/wp-content/uploads/2015/07/Sales_France_ surveillance_legislation_analysis_0715.pdf.

surveillance measures.[116] Another argument the French government could make is that the Prime Minister is elected by the people, and the democratic process is a powerful check on the abuse of authority. In short, if the people do not want to have this law, they should go through democratic means to get it removed. Since the Prime Minister and the people's elected representatives in Parliament overwhelmingly support this piece of legislation, the European Union should respect the decisions of the French government.

The European Court of Justice will probably find the lack of oversight is the greatest weakness in the *Loi Relative au Renseignement*. Although the French government can make several compelling arguments, the National Committee of Intelligence Techniques Control's lack of enforcement power and the absence of any judicial authority could allow arbitrary abuse of an individual's right to privacy. Also, democracy is a powerful tool in ensuring people have an avenue to participate in government, but the democratic process is not perfect. So, individuals need an independent judiciary to protect the rights of people who may not be in the majority.

B. Does the French Law Violate Article 8?

The next issue the European Court of Justice will have to analyze is whether the *Loi Relative au Renseignement* is in violation of Article 8 of the ECFR. Article 8 says everyone has a right to protection of personal data, and that data has to be processed fairly for specific purposes on the basis of consent or a legitimate law.[117] Also, people have a right to access data collected and a right to have incorrect data rectified.[118]

The major issue the European Court of Justice will have to analyze in regard to the *Loi Relative au Renseignement* is this law's procedure. Article 8's primary focus is on the process by which the data is collected.[119] The court has held previously and research suggests that data can be collected in vast amounts if the process is fair and there are adequate safeguards to prevent abuse.[120] The European Court of Justice will likely find that this vast data collection, without discrimination, is not a fair process of surveillance, and this law violates Article 8 of the ECFR.

---

[116] Conseil constitutionnel [CC] [Constitutional Court] decision No. 2015-713 DC, July 23, 2015, J.O. 0171 (Fr.).

[117] EU Charter of Fundamental Rights (ECFR) No. 2000/C of December 18, 2000, art. 8, 2010 O.J. (C 364) 10.

[118] *Id.*

[119] *Id.*

[120] E.U. Network of Independent Experts in Fundamental Rights, Commentary of the Charter of Fundamental Rights of the European Union, at 95 (2000), http://ec.0000000europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf.

1. Right of Access

The right of access to one's personal data is specifically mentioned in Article 8(2) of the ECFR.[121] The right to know one's data is being processed and the right to challenge the validity of the government's collections of data is an integral part of the right to protection of personal data.

The Commission will likely argue a major issue with the French law is that the process of mass surveillance is not fair because the information is being processed without the knowledge or consent of the subjects of surveillance. The law does not provide any avenues for French citizens to know what data is being collected or put through the government's algorithm. The European Commission may use the holding of the European Court of Justice in *Digital Rights Ireland Ltd. v. Minister of Communications* by arguing that the court paid special attention to the fact the subjects of surveillance themselves would not be aware they were being analyzed by intelligence agencies and therefore could not argue to any legitimate authority that their data was being processed unfairly or without cause.[122] Without such knowledge, individuals do not have a legitimate way to defend themselves if the government decides to implement more intrusive surveillance measures.

The French government will likely reply by arguing that the law was originally designed to combat terrorism.[123] Allowing everyone to know what data is being collected and when an individual is subject to more intrusive surveillance measures would undermine the purpose of the law. If people could bring claims against the French government, potential terrorists would eventually learn how to conduct their illegal activities around the protection of the algorithm. The more information there is available about how the French government conducts their secret surveillance, the more likely it would be that terrorist threats could exploit this information to hurt French citizens. Further, there *is* an avenue where a person can simply request information about whether the National Committee of Intelligence Techniques Control has engaged in intrusive methods on a person

---

[121] EU Charter of Fundamental Rights (ECFR) No. 2000/C of December 18, 2000, art. 8, 2010 O.J. (C 364) 10.

[122] Case C-293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Celex No. 612CJ0293, European Court Reports (Apr. 8, 2014).

[123] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912 of July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735.

individually.[124] Although this does not allow for instant right of access, a person does still have an avenue to seek redress.

2. Specificity

The Commission could also argue that the data is not being collected for specific purposes and does not allow for any sort of exceptions. For example, the law does not allow exceptions for journalists who may have private information about anonymous sources.[125] This information will also be collected and potentially analyzed without discernment from other data.[126] Another example of the lack of discrimination is potential communications between clients and their attorneys.[127] As technology has progressed, many lawyers have turned to the internet to communicate more efficiently with their clients. This law potentially puts confidential attorney-client communications in the government's possession. In the case of the *Loi Relative au Renseignement*, these potentially confidential discussions will also be subject to the surveillance law and can be monitored by the government without the consent of surveillance subjects. This is a violation of a person's rights under Article 8 because the law is not specific enough to take these especially serious privacy concerns into account.[128] The generality of the surveillance law subjects individuals to arbitrary enforcement; therefore, it violates Article 8 of the Charter.

The French government could respond to this argument in several ways. They could claim the collection of metadata is a nominal invasion of privacy rights because the data will not be used unless they meet certain qualifications required by the algorithm. Further, by using an algorithm as a specific discriminatory filter, intelligence services are prevented from engaging in unfair surveillance practices. In short, the French government is directly targeting potential terrorist threats from metadata.

The French government can also argue that metadata is a specific type of data, and this targeted approach shows the government's intent to only look

---

[124] *Id.* art. 833-2.

[125] NATHAN A. SALES, FRENCH SURVEILLENCE LAW COMAPRED TO U.S. SURVEILLENCE LAW (July 31, 2015), http://insct.syr.edu/wp-content/uploads/2015/07/Sales _France_ surveillance_ legislation_analysis_0715.pdf. *See also* Conseil Constitutionnel [CC] [Constitutional Court] decision No. 2015-71 DC, July 23 2015, J.O. 0171 (Fr.), at 28.

[126] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912 of July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735 art. 821-7.

[127] *Id.*

[128] Comm. of the Charter of Fundamental Rts. of the European Union, at 95 (2000), http:// ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf.

at certain data for a specific reason. Metadata is a description of actual data, and metadata alone does not tell an individual much unless they are processed to the point where they actually recreate what is essentially a copy of a person's personal data.[129] The French government is not going to be putting raw data together unless: first, the algorithm indicates the subject of surveillance is a potential threat to the French people; second, the National Committee of Intelligence Techniques Control gives an opinion on whether more serious surveillance methods should be used; and third, the Prime Minister renders a final decision that, based off the data collected, an individual poses a terrorist threat.

The European Court of Justice will probably find this to be one of the more difficult issues to analyze, but in the end, it should find the collection and processing of metadata does violate Article 8. The use of metadata for security purposes is a relatively new phenomenon in comparison to more traditional methods of surveillance such as wiretaps, videotaping, and even hacking into individual's computers to read e-mails. The European Court of Justice may take a new approach and find metadata is too unsophisticated to be considered in the same category as personal data. Although having access to an individual's metadata creates the potential for state abuse, this potential may not become a reality, because the law indicates that metadata will exclusively be used for the purpose of stopping terrorism.[130]

By accepting this argument, the European Court of Justice would have to overcome the logic that it utilized in *Digital Rights Ireland Ltd. v. Minister of Communications*, when it held that the storage of metadata did violate an individual's privacy rights because it allowed for the potential to create personal data.[131] This indicates that metadata can be considered personal data in that they can be used to link raw information to a particular individual. Even though the algorithm acts as a filter, simply having access to data capable of being manifested into information that can be directed at an individual in particular is still a violation of Article 8.

---

[129] Jenn Riley, *Understanding Metadata*, NATIONAL INFORMATION STANDARDS ORGANIZATION 2017, http://www.niso.org/publications/press/UnderstandingMetadata.pdf.

[130] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912, July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735 822-2.

[131] Case C-293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Celex No. 612CJ0293, European Court Reports (Apr. 8, 2014).

3. Independent Authority

Article 8(3) of the ECFR says compliance with Article 8 by an independent authority is also a fundamental right.[132] Accordingly, another argument the European Commission could make is that the National Committee of Intelligence Techniques Control is not an independent authority that controls the French government's surveillance. Although the French law does try to ensure the board is independent by taking actions such as term limits, proportional representation based off of political parties and gender, and ensuring two judges are on the panels at all times, the *Loi Relative au Renseignement* fails to give the National Committee of Intelligence Techniques Control any authority in the surveillance decisions.[133]

When it comes to this argument, France would have difficulty trying to convince the European Court of Justice that a capable independent body exists to control the government's use of surveillance, as required in Article 8(3) of the ECFR. Therefore, at this point France may have to turn to some of the exceptions that are indicated in Directive 95/46/EC.

C. Does the Law Meet any Exceptions?

Directive 95/46/EC provides that under certain circumstances a government can be allowed to collect an individual's personal data and infringe on an individual's right to privacy. These exceptions include national security purposes, defense, public security, prosecution of criminal offenses, and certain economic interests of the state.[134] In order to use these exceptions to justify infringement on an individual's personal rights, however, the government must balance the interests of the state and of the individual when creating laws. If the European Court of Justice does hear a claim brought by the European Commission, the court will have to implement this balancing test.

France will argue that the *Loi Relative au Renseignement* is designed to combat a real and active terrorist threat that puts the country's citizens in danger. The law specifically states that it is designed to prevent terrorist

---

[132] EU Charter of Fundamental Rights (ECFR) No. 2000/C of December 18, 2000, art. 8, 2010 O.J. C 364 at 10.

[133] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912, July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735 art. 801-1.

[134] Directive 95/46/EC, of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31-50.

attacks on government institutions and the French public.[135] It is also designed to prevent organized crime and the proliferation of weapons of mass destruction.[136] The goal of the law is focused and designed to prevent harm to French citizens. So, the French government is justified in implementing the contents of this law in order to keep the French people safe from this mounting threat.

France will likely claim that in this past year France has experienced a rise in terrorist attacks, and France is perpetually exposed to radical individuals who threaten the French way of life.[137] After the *Charlie Hebdo* attacks of January 2015 there was another terrorist attack on November 13, 2015. The latter was the deadliest yet, resulting in over a hundred civilian casualties. The original threat that was used as justification to pass the *Loi Relative au Renseignement* has manifested into a reality that will forever change how France addresses terrorism.

The issue of modern terrorism causes concerns for France because the internet is now being used by terrorist organizations like the Islamic State of Iraq and the Levant to recruit cyberjihadists from around the world.[138] The French government could further state that the fight against terrorism is unique and requires a different method of defense than traditional armed conflicts. Unlike conflicts between countries, the conflict between terrorist organizations and the French public does not involve formal military units. In this case, terrorists can be people who have no military experience, living seemingly innocuous lives.

The nature of this kind of conflict makes it difficult for governments to detect threats before they happen. It is also more severe than traditional armed conflict because the intended targets of terrorist attacks are civilians, and the individual terrorists often reside, in some capacity, in the state they wish to attack. Consequently, more innovative measures, like the ones implemented in the *Loi Relative au Renseignement*, are necessary to thwart the plots of individuals who are determined to put an end to the French way of life.

France can also argue that it *did* take into account individual liberties, because France recognizes that implementing new security measures often

---

[135] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912, July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735 art. 811-3.

[136] *Id.*

[137] *Terrorisme: "Nous devons nous préparer à d'autres assauts," prévient François Hollande*, L'EXPRESS, (Aug. 8, 2015), http://www.lexpress.fr/actualite/societe/attentats-nous-devons-nous-preparer-a-d-autres-assauts-estime-francois-hollande_1709336.html.

[138] *Cazeneuve appellee les géants de l'internet à lutter contre le terrorisme*, FRANCE TV INFO AVEC AFP (Feb. 20, 2015), http://www.francetvinfo.fr/monde/terrorisme-djhadistes/cazeneuve-appelle-lels-geants-de-I-internet-a-luttercontre-le-terrorisme_829523.html.

calls for reassurance by the government that this new power will be curtailed by procedural and judicial safeguards. One of the measures the French government has taken is forbidding the government from monitoring French people with regard to politics, public debate, and the media.[139] The law also allows French people to seek redress through the French court system if they believe the surveillance measures used on their personal data were unjustified.[140] In short, France would answer by drawing attention to the fact that the *Loi Relative au Renseignement* does seek to strike a balance in the freedom versus security dilemma that has plagued democracies since their inceptions.

France will likely say that it did take individual liberty interests into account when creating this law, but in this case because the security interest is so serious, an individual's liberty interest must make some space to allow for protection of the public welfare. The rise of technology has pressured governments to take more serious measures to protect their citizens, and perhaps using the technology—for instance by the use of algorithms—is the best way to combat the technology used to perpetuate violence.

It seems unlikely that the European Commission will bring a case against the government of France considering how recent the 13/11 terrorist attacks took place. Further, the European Commission may have a stronger argument for removing the *Loi Relative au Renseignment* if it waits until after France is no longer in a state of emergency. Regardless of when the European Commission brings suit, it will have compelling arguments regarding the disproportionate effects on law abiding citizens and the lack of safeguards of this law.

The European Commission will respond by acknowledging that the security concern is a legitimate interest, but that France's method of combatting terrorism has a disproportionate effect on the French public, one that renders the law unjustifiable and violates Articles 7 and 8 of the ECFR. Although there are exceptions to Directive 95/46/EC, these exceptions must be weighed against, and only implemented in light of, the seven principles needed to collect an individual's personal data. These seven principles are: there must be notice of collection of personal data, the collection must be for a legitimate purpose, the subject of data must give their consent, the data collected should be secure, the subject of collection should know who has his or her information, the subject should also have access to their data, and any

---

[139] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912 of July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735.

[140] *Id.* at 706-25-12.

organizations violating these principles should be held accountable.[141] The European Commission will argue that the French government failed to balance these seven principles. The law does not give the subject of the surveillance notice of collection of data when the government implements more intrusive surveillance measures. Although the subject of the collection can appeal the surveillance measures, the subject would have no reason to believe the government is implementing these more serious measures unless the person was able to discover this on his or her own.[142] A grave shortcoming of the *Loi Relative au Renseignement* is that the law does not seem to mitigate this notification principle.

Also, the law does not ask for the surveillance subject's consent before processing that person's data. This expansive government policy collects all French internet users' data, and then the Prime Minister determines if additional surveillance techniques need to be applied. The French government could argue that it had the consent of the people to create this law democratically. This would not be a compelling argument because of the public opposition, and one cannot get consent to violate an individual's fundamental rights through a representative in the legislature.

The European Commission will also argue that a major flaw of this law is that there are several principles that are not addressed. The law fails to discuss how it will ensure that the data collected will be secured or what agencies will have access to the data besides the Prime Minister and the National Committee of Intelligence Techniques Control.[143] These failures to legislate particularities in regard to these principles call into question the fairness of a law that proposes searching for a small minority of people who may be potential internet using terrorists by monitoring the French public indiscriminately.

The lack of judicial control over the Prime Minister's decisions gives him control over a large amount of data with no check on his authority. The *Loi Relative au Renseignement* indicates that the Prime Minister can exclusively use the information gathered through the algorithms in order to combat terrorist threats, but if the Prime Minister chooses to use this information for more illegitimate purposes there is no system in place to hold him accountable.[144]

---

[141] Parliament and Council Directive 95/46, art. 7, 1995 O.J. (L 281).

[142] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912 of July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735 art. 833-2; this provision indicates that a person has a right to appeal surveillance techniques used on them and the ability to correct incorrect data.

[143] *Id.* art. 773-2; this provision addresses generally who will have access to the collected data but does not name specific committees or who is responsible for supervising said committees.

[144] *Id.* arts. 833-2, -3. These articles indicate the Prime Minister's scope of authority, but do not discuss any checks on the Prime Minister's power.

The National Committee of Intelligence Techniques Control is an ineffective group to hold the Prime Minister accountable or limit the scope of the surveillance techniques because its decisions have no binding authority. Further, the decisions of the Prime Minster and the recommendations of the National Committee of Intelligence Techniques Control are considered state secrets. According to the law the French people are required to receive a yearly report in which the National Committee of Intelligence Techniques Control reveals how many times the more serious surveillance techniques are used by intelligence services.[145] The law fails in specificity because there is never any disclosure of who the techniques were used upon, what evidence was used to determine these additional measures were necessary, or whether the use of these techniques were implemented for political motivations.[146]

The European Commission will likely argue that the lack of effective judicial safeguards makes this law in violation of the ECFR, even when the public and national security exception is brought into play. The threat of terrorism is a part of governance; all governments are potential targets of terrorist attacks, and the risk of terrorism is a part of ruling and living in modern society. This threat cannot be used as a justification to forgo the foundations of the European Union, and cannot be used to compromise the fundamental freedoms of privacy and protection of personal data.

D. Will the Law be Upheld under the Margin of Appreciation Doctrine?

At this point the European Court of Justice will likely have to conduct a margin of appreciation analysis. The margin of appreciation doctrine allows members of the European Union to have some latitude when it comes to developing state policy in order to implement European Union laws.[147] As mentioned previously, the European courts often allow for a wide margin of appreciation under certain circumstances. France will likely say it should have a larger margin of appreciation because the *Loi Relative au Renseignement* was created for national security purposes.[148] The European Commission will probably reply by saying the court should use a narrower margin of appreciation because the law compromises a person's absolute rights and seeks to regulate an intimate aspect of private life.[149]

In the end, their arguments will still come down to one issue: whether the *Loi Relative au Renseignement* encroaches on the fundamental rights

---

[145] *Id.* art. 833-9.
[146] *Id.*
[147] GRUSZCZYNSKI & WERNER, *supra* note 101, at 240–42.
[148] *Id.*
[149] *Id.*

guaranteed in Articles 7 and 8 of the ECFR beyond what is permitted under the margin of appreciation doctrine to violate France's obligations under the ECFR. All things considered, the European Court of Justice will likely find that even with the margin of appreciation as a means for more flexibility with member states, there are still insufficient safeguards to protect French citizens' fundamental rights. The previously mentioned case law indicates that if there is a clear communication of how the data will be used, and there is a proper independent mechanism for review, then it will likely not violate a member state's obligations to the European Union.

The European Court of Justice may consider offering suggestions to the French government on how to mitigate the *Loi Relative au Renseignement*'s encroachment on civil liberties. One way the court could do this would be by suggesting that the French government make the National Committee of Intelligence Techniques Control a body that can make binding decision regarding whether surveillance techniques should be increased. The French law has a lot of details to ensure that this body is independent. The committee requires the equal representation of men and women, it includes two judges, and the members have specific term limits.[150] It even includes a person who is an expert in electronic communications.[151] These facts seem to indicate that this committee is qualified to make decisions independently, and perhaps they should be given more substantive authority to act as a check on the Prime Minister's authority. This body could act as a judicial authority which could afford citizens protection for their fundamental rights because there is some additional safeguard in managing their personal information.[152]

Another recommendation the European Court of Justice could offer is to reprogram the algorithm to consider extremely private information, such as conversations between lawyers and their clients, doctors and their patients, and journalists and their sources. The makeup of the algorithm is highly sophisticated and largely unknown. But, perhaps an additional safeguard for personal data would be to simply redesign a part of the algorithm so as to exclude the processing and collecting of this kind of information. This

---

[150] Loi 2015-912 du 24 juillet 2015 de relative au renseignement [Law 2015-912 of July 24, 2015 Relating to Intelligence], JOURNAL OFFICIAL DE LA RÉPUBLIQUE FRANÇAISE [J.O.], July 26, 2015, p. 12735 art. 831-1.

[151] *Id.*

[152] A similar court, known as the United States Foreign Intelligence Surveillance Court, has been used in the United States to act as some safeguard to a person's personal data. Though it is imperfect, this court does provide some additional measures to ensure the fair usage of a person's private information. ELIZABETH B. BAZAN, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions*, CONGRESSIONAL RESEARCH SERVICE RL30465 (2007), https://www.fas.org/sgp/crs/intel/RL30465.pdf.

would allow French citizens to have greater solace, knowing some personal information cannot be collected or used by the French government.

Finally, the European Court of Justice could advise France not to implement its system of mass surveillance, and only use the algorithm to collect an individual's metadata if there is other evidence to suggest this individual poses a terrorist threat. The French government is unlikely to favor this option, which would allow it to conduct surveillance measures on a small segment of the population. France would argue this would not afford any additional protection beyond the bounds of law before the implementation of the *Loi Relative au Renseignement*.

V. CONCLUSION

Balancing interests of freedom and security has been an ongoing issue in democracies, and it only gets more complicated with the advent of modern technology. The *Loi Relative au Renseignement* illustrates this dilemma. With the recent attacks on French citizens, it is not surprising that the French government feels pressure to protect its people. It is clear some action must be taken in order to protect individuals from terrorist attacks while also staying true to the democratic and individualistic values that formed the foundations of the modern French government.

The European Court of Justice will likely be equally concerned with maintaining the balance between freedom and security. Considering all of the external resources, however, the court will likely find that the *Loi Relative au Renseignement* comes into significant conflict with the ECFR. The text of Articles 7 and 8 of the ECFR, as well as the subsequent case law, suggest a broad interpretation of the rights that these Articles offer.

Another tool the court can use to help make its decision in regard to this law is the legislation passed by the European Union. These documents lay out specific criteria in which data can be taken, stored, and used. They also talk about under which circumstances the government can collect information without following the recommended criteria.

Finally, the European Court of Justice will use cases decided by the European Court of Human Rights. The European Court of Human Rights holds special value to the European Court of Justice, and their decisions should guide the European Court of Justice to the conclusion that France should take additional steps to mitigate the negative effects on its citizens' fundamental rights in order to bring France into compliance with its European Union obligations.