A COMPARATIVE STUDY ON SURVEILLANCE AND PRIVACY REGULATIONS (THE UAE VS. THE USA AND THE EU)

Ibrahim Sulieman Al Qatawneh [*], Wesam Almobaideen [**], Mohammad Qatawneh [***]

* College of Law, Al Ain University, Al Ain, the UAE
** Rochester Institute of Technology, Dubai, the UAE; Department of Computer Science, The University of Jordan, Amman, Jordan
*** *Corresponding author*, Department of Computer Science, The University of Jordan, Amman, Jordan
Contact details: The University of Jordan, Queen Rania St, Amman 11942, Jordan

OPEN ACCESS

How to cite this paper: Al Qatawneh, I. S., Almobaideen, W., & Qatawneh, M. (2022). A comparative study on surveillance and privacy regulations (the UAE vs. the USA and the EU). *Journal of Governance & Regulation, 11*(1), 20–26. https://doi.org/10.22495/jgrv11i1art2

ISSN Print: 2220-9352
ISSN Online: 2306-6784

Received: 23.07.2021
Accepted: 03.01.2022

JEL Classification: K24, L50
DOI: 10.22495/jgrv11i1art2

Abstract

Surveillance is becoming the norm in today's life, especially with the pandemic of COVID-19. Surveillance of public crowds and activity is a controversial issue that can contradict the privacy of individuals (Federal Decree-Law No. (5) of 2012). This paper presents a comparative study of surveillance and privacy regulations and law in the UAE compared to the USA and the EU. The objective of this comparison is to highlight the amendments that have been adopted to improve laws and regulations, the need for further improvement, and the strengths and weaknesses in each of these countries. A discussion of different acts adopted in these countries and comparing them can help security experts to cooperate with legislators in order to rectify shortcomings and improve the acts adopted in their respective countries. Furthermore, we think that such a comparison can help system developers to find an easier way to accommodate the differences in security measures that they have to tackle and incorporate when they are serving customers in these countries and especially in the UAE. A legal framework has been proposed in order to define the maturity level of regulations adopted by a government in regard to surveillance and privacy laws and acts.

Keywords: Surveillance and Privacy, Regulations, Cyber Law, Privatization Policy, Regional Government Analysis

Authors' individual contribution: Conceptualization — I.S.A.Q., W.A., and M.Q.; Methodology — I.S.A.Q., W.A., and M.Q.; Validation — I.S.A.Q., W.A., and M.Q.; Investigation — I.S.A.Q., W.A., and M.Q.; Resources — I.S.A.Q., W.A., and M.Q.; Data Curation — I.S.A.Q., W.A., and M.Q.; Writing — Original Draft — I.S.A.Q., W.A., and M.Q.; Writing — Review & Editing — I.S.A.Q., W.A., and M.Q.; Visualization — I.S.A.Q., W.A., and M.Q.; Supervision — I.S.A.Q.; Project Administration — I.S.A.Q. and M.Q.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

1. INTRODUCTION

According to the Foreign Intelligence Surveillance Act (FISA) (Bazan, 2007), surveillance is defined as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs within the United States"[1]. Therefore, electronic surveillance includes the use of

[1] https://www.law.cornell.edu/uscode/text/50/1801

mechanical, electronic or any other surveillance device of the contents of wire or electronic communication, without the willing agreement of a party to the communication who has a reasonable expectation of privacy. Contents of a communication can be any information related to the identity of the communicating parties, or their existence, purport, substance, or meaning of the communication.

Surveillance can be done on the wire when the data is being transferred from a source point to a destination point over a wire, a cable, or other communication channels via wiretapping, bugging, or videotaping. Alternatively, it can be done through electronic communication like email, VoIP, or accessing data uploaded to the cloud. Geolocation tracking is yet another way to do surveillance through GPS, cell-site data, or even radio-frequency identification (RFID) (Open Institute of Information, n.d.-a).

The meaning of the term "privacy" depends on the legal context. In constitutional law, privacy is associated with self-determination and autonomy and means to have the right to make a person the ability to own decisions regarding inherently personal issues without government intimidation, coercion, or regulation. In the context of common law, privacy is associated with isolation or seclusion and means to have the right to live alone. Under statutory law, privacy is linked to secrecy and implies the right to be protected against nonconsensual disclosure of private or confidential sensitive information (U. S. Department of Justice, n.d.).

Several corporations and organizations are declaring to be noncommercial and claim that they maintain the privacy of users, but in fact, they use some samples of our data to study our behavior, desires, and interests for many things, and this is a major breach of the users' privacy (Braga, 2014).

The conflict between the need for surveillance to protect the countries' and nations' security and the need to protect the personal right of privacy is an ongoing battle. Therefore, every country that has established standards has also established mechanisms to enforce those standards. Surveillance, in this regard, is a necessary tool that disregards the privacy of individuals to protect the rights of other individuals and groups. Any discussion about the issue of surveillance must recognize this reality. Parents watch children and employers watch employees (K.N.C., 2019).

In the United States, the architects of the Constitution strove for a degree of harmony between the competing values of privacy and surveillance. Nevertheless, we need to recall the technological realities of the late eighteenth century. When Madison wrote the Bill of Rights, the sound could not yet be transmitted or recorded. The only means of penetrating private spaces were eavesdropping and physical trespass, and so those acts were constrained under the strict warrant controls of the Fourth Amendment (K.N.C., 2019).

To address this conflict FISA has established the Foreign Intelligence Surveillance Court (FISC) and the Court of Review that manage applications submitted to the court in order to authorize the use of certain devices for electronic surveillance. FISC deals with the decisions of applications regarding "electronic surveillance, physical searches, pen registers or trap and trace devices, or orders for production of tangible things anywhere within the United States under FISA (U. S. Department of Justice, n.d.). If an application is rejected by FISC then the Court of Review becomes responsible for reviewing that application.

Electronic surveillance is a search under the Fourth Amendment (Open Institute of Information, n.d.-b), which provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". Therefore, warrant requirements similar to other searches are needed for surveillance. To approve a warrant or surveillance request application by the FISC under FISA, the government has to show that the suspect to be kept under surveillance must have committed some kind of suspicious activity or must have been involved in violations of the criminal law, particularly when that action includes a foreign threat to the national security of the certain country (Bazan, 2007).

The purpose of this paper is to provide researchers in cybersecurity and legal fields with a comparison between laws and acts that have been adopted in the USA, the EU, and the UAE and that are related to surveillance and privacy issues. The reason behind choosing these counties is the high maturity level of cyber laws in the USA and the EU on one hand. On the other hand, we believe that the UAE represents a model for other nations in terms of the fast pace of improving the life quality of citizens and residents along many axes including policies and law.

This comparison would highlight the amendments that have been adopted to improve laws in each of these countries, the need for further improvement, and the strengths and weaknesses in each. A discussion of different acts adopted in these countries and comparing them can help security experts to cooperate with legislators in order to rectify shortcomings and improve the acts adopted in their respective countries. Furthermore, we think that such a comparison can help system developers to find an easier way to accommodate the differences in security measures that they have to tackle and incorporate when they are serving customers in these countries.

The rest of this paper is organized as follows. Section 2 presents the literature review of some studies published in the area of privacy and surveillance. In Section 3, we discuss the methodology that has been followed in conducting the research in this paper and the proposed legal framework. Results are presented in Section 4, which focuses on specific observations and recommendations. In Section 5, we discuss various features of surveillance and privacy laws and compare these laws and policies adopted in the USA, the EU, and the UAE. Section 6 concludes the paper.

2. LITERATURE REVIEW

Several research papers have been proposed to address the issue of law and policies in regards to surveillance and privacy in many countries. This is because the issue of drawing the bounds of surveillance and privacy is considered as one of the most important challenges of our new digital life. At the same time, people need more and better

protection over their personal information and data, which led to the emergence of conflict between the need for surveillance to protect society's security and to take this issue into consideration for protecting personal privacy.

Cyber security law in the UAE is one of the most advanced and continuously improved ones in the Middle East and other neighboring countries. For example, the Emirate of Dubai has adopted the "Dubai Cyber Think Tank" initiative, which has been launched by Dubai Electronic Security Center (DESC) (2017). This initiative allows public and private sector entities to carry out research, have discussions, brainstorm ideas, and come out with recommendations to address cybersecurity issues. There are several priorities of the work included in this initiative as participating in the development of policies and framework that strengthen the cybersecurity of Dubai, and facing and mitigating the current and future risks and challenges related to cyber security for the public and private sector.

This initiative focuses on a set of core domains that are part of the DESC's (2017) Dubai Cyber Security Strategy, which supports future plans of Dubai in the realm of cyber security. These domains include the following points ordered relative to the importance of the topic in this paper:

- "Ensuring data privacy for the public and private sectors and individuals.
- Putting controls in place to protect data confidentiality, integrity, and availability.
- Establishing national and international collaboration to manage cyber risks.
- Achieving awareness, skills, and capabilities to manage cybersecurity risks in the public and private sector.
- Promoting research and development in cybersecurity.
- Ensuring the continuity and availability of IT systems".

The Global Cyber Security Capacity Centre (2016) proposed a legal framework to address various aspects of security-related issues. The most relevant aspect to this study is "Privacy, Freedom of Speech & Other Human Rights Online". The study classifies the readiness toward each aspect according to a five-scale measure. The scales are Start-up, Formative, Established, Strategic, and Dynamic. Up to the authors' knowledge gained through the literature survey that was conducted, there is no previous work that compares policies and laws in the cybersecurity area between the USA, the EU, and the UAE with the focus on surveillance and privacy. This comparison is needed to address the strengths and weaknesses in the laws of these counties and especially to help legislators and lawmakers in the UAE to address the improvements that can be considered in order to reach the level of cyber law maturity in the other two countries.

In Adams (2020), the author discussed two issues: the first one is how digital surveillance forms a problem for workers in the field of journalism and the second one is the effect of transformation to digital distribution on the content of events, news, and reports. In addition, the author mentioned that the process of transformation to digital distribution drove the publishers to gather and share data with other publishers. The author proposed many recommendations to tackle such issues through a high level of transparency.

Another important study provided by Abokhodair, Abbar, Vieweg, and Mejova (2017), focuses on online privacy in Saudi Arabia and Qatar. The study shows that Saudi Arabian and Qatari believe that privacy comes from the Islamic religion, and there is a need to protect personal privacy.

The authors (Goldberg, Johnson, & Shriver, 2019) mentioned that the EU began applying a set of regulations, which protect the personal data rights of the EU citizens by setting a set of rules for companies to regulate the process of exchanging personal information among themselves. In addition, the authors discussed the effect of such rules on e-commerce websites in the EU.

To address the issue of accessing and using personal data by smartphone developers in many other applications, Li et al. (2017) proposed a new framework called "PrivacyStreams" to manage the process of accessing personal data. The results showed that this framework can protect sensitive mobile data.

Rachovitsa (2017) discussed the issue of protecting online privacy and mentioned that online privacy can be protected by enhancing the internet standards and using and designing different technological tools, which support and complement the existed legal frameworks.

Chen, Beaudoin, and Hong (2016) proposed a new model, which is inspired by negative privacy experiences and comprises three stages. The aim of the proposed model were to explore and discuss the internet users' behaviours regarding the issue of personal data privacy in order to enhance and protect online privacy.

Since the issue of data privacy is important and considered a human right, the United Nations has put it on its agenda. Zalnieriute (2015) discussed the possibility of making privacy a legal rule under international law through discussion of different perspectives of data privacy.

3. METHODOLOGY

In this research, the authors adopted the comparative approach based on analyzing the legislative provisions that dealt with surveillance and privacy law UAE legislation and comparing it with USA and EU legislations. This paper also proposed a framework to analyze the maturity level of legislation in any country and provides recommendations for the adoption of new rules for regulating surveillance and privacy. Specifically, the authors compared laws in these three countries and regions of the world based on data collected from research papers and websites that represent legislatures and legal bodies in these countries.

The researchers use specific comparative approach in legal research to analyze the existence and maturity level of legal acts and laws related to surveillance and privacy in the targeted regions. The main method used focuses on the existence of the law and then compare them, if exist, to tackle specific dimension or a need expressed in terms of questions as can be seen in Table 2.

The authors began collecting data regarding surveillance and privacy in the fall of 2020. The most relevant data was collected from many official sources in the USA, the EU, and the UAE. Other several ideas of surveillance and privacy were gathered from journal articles, and master's theses.

A proposed legal framework for the maturity of surveillance and privacy acts

We propose a legal framework that is inspired by the work done by The Global Cyber Security Capacity Centre (2016). We use the same scale presented in that work so the maturity of the surveillance and privacy law will be as Start-up, Formative, Established, Strategic, and Dynamic. Table 1 distinguishes these levels.

Table 1. Level of maturity

Level of maturity	*Definition*
Start-up	There is no domestic law that targets privacy and surveillance issues.
	Discussions of privacy surveillance-related policies by multiple stakeholders may have begun but did not result in concrete legislation or standards.
Formative	There are partial domestic rules that target the privacy and surveillance issues, how intelligence services deal with privacy and surveillance, how does the government controls these issues, how companies cooperate with intelligence services and the government in regards to these issues.
	Discussions of privacy surveillance-related policies by multiple stakeholders may have begun but did not result in concrete legislation or standards.
	Stakeholders representing key sectors in the country have been consulted for the development of legislation addressing human rights online.
Established	Domestic law recognises fundamental human rights on the internet, including privacy online, and defines specific policies of surveillance, defining the right of a human to be informed of the existence of such surveillance.
	Domestic law follows international standards and takes precautions to protect the individual's right to privacy during the surveillance.
	Actors from the government and private sector are involved in specifying the laws and regulations on privacy and surveillance.
Strategic	International and regional standards and known good practices are used in the assessment and amendment of domestic legal frameworks related to privacy and surveillance.
	In order to exceed the acceptable level specified in international standards, research and proper measures are used to evaluate the effect of current rules and policies regarding surveillance and privacy.
Dynamic	Due to the very dynamic and constant changes in the application of technology of communication and surveillance, procedures have been adopted to control the amendment policies and laws related to surveillance and privacy.
	The country fully recognizes that access to internet communication channels is a fundamental human right. The country contributes actively to the global interaction for surveillance and privacy, especially on the internet. Domestic stakeholders participate actively to shape related domestic and international standards.

4. RESULTS

In this section, we would like to highlight the following observations and recommendations.

Observation 1: The UAE and the USA have more than one surveillance and privacy-related laws, in contrast to the common and General Data Protection Regulation (GDPR) law adopted in the EU.

Recommendation 1: It is recommended to have one general and comprehensive federal law that governs surveillance and data privacy issues in the UAE in order to have one common reference law. This does not mean that more specific law, which respects the general one, cannot be adopted in order to impose more specific requirements such as the case with fostering and protecting economic prosperity.

Observation 2: The authors believe that no law in the three considered countries/regions has reached the maturity level of Strategic or Dynamic according to the proposed legal framework presented in Section 3.

Recommendation 2: Legislatures in these countries/regions should consider the improvement of law related to surveillance and privacy in order to reach the Strategic level of maturity or even the Dynamic one which allows these laws and acts to adapt to new technologies and other external factors.

5. DISCUSSION

There is no comprehensive federal-level data privacy and protection law in the UAE. However, at the emirates level, there are laws that govern data security and privacy laws in the UAE. Additionally, data protection articles have been introduced into some sector-specific laws and into the laws that control the work of sector-free or special economic zones, such as Dubai International Financial Centre, the Abu Dhabi Global Market, and the Dubai Health Care City.

The new Dubai International Financial Centre (DIFC) Law No. 5 of 2020 Data Protection Law (DPL) (Wilkinson & Gibson, 2020) replaces the DIFC Law No. 1 of 2007 Data Protection Law (DESC, 2017) and allows the DIFC to be more closely aligned with GDPR law that is applicable in Europe (European Union, 2016). GDPR is applied across the EU and this represents a major difference compared to the USA and the UAE where there is more than one law which makes it difficult in some cases to decide on the law that should be applied.

Article 379 of the UAE Penal Code can be considered as the privacy law which is most relevant to a general application in the UAE which prevents the use or dissemination of secret data by a person who can access this data according to a profession, craft, situation or art. Any disclosure of such secret data should be based on the consent of its owner, or otherwise in accordance with the law.

Another issue that is related to surveillance and privacy is the focus of the operation done by intelligent services according to the adopted laws. This focus could be on national security, economic, or other matters. In the UAE, we can see that most of the currently adopted laws are focused on economic aspects. This is evident by the existence of the following laws:

1. DIFC Law No. 5 of 2020 Data Protection Law (DESC, 2017).

2. Regulating Telecommunications (Federal Law by Decree 3 of 2003 as amended). This consists of regulations or policies enacted by the Telecoms Regulatory Authority (TRA) in regards to data protection of the UAE telecoms consumers.

3. The Use of the Information and Communication Technology (ICT) in Health Fields (ICT Health Law) was issued on February 6, 2018, Federal Law No. 2 of 2018.

4. The UAE Central Bank issued on September 30, 2020, a new Stored Value Facilities Regulation (SVF Regulation), repealing and replacing the Regulatory Framework for Stored Values and Electronic Payment Systems issued in September 2016.

The number of laws related to economic sectors and the continuous improvement of these laws prove the interest of the UAE in protecting the economic prosperity of the country. In the USA, intelligent services are not used for specific economic reasons which is the same case with most EU countries.

The way through which intelligent services force companies to allow access to private data is different in the three considered countries/regions. In the UAE, this is provided in the Federal Decree-Law No. (5) of 2012 on combating cybercrimes, which provides that "The officials determined by a decision from the Minister of Justice shall have the capacity of judicial officers for the ascertainment of acts committed in violation to the provisions of this Decree-Law, and the competent authorities in the Emirates are required to submit facilities necessary to those officials to enable them to perform their tasks" (Article 49). In the USA, this is provided by warrants, subpoenas, and court orders while in the EU, each country has its own way of enforcing this kind of compliance. Table 2 lists a set of questions presented by DESC (2017). For each of these questions, we present the current situation in the UAE constitution and law, the associated recommendation, and compare the UAE case with that of the USA and the EU in the last column.

Table 2. List of questions (Part 1)

Questions	***Current situation in the UAE***	***Recommendations***	***Current situation in the USA and the EU***
How can intelligence services compel companies to provide access to data?	Federal Decree-Law No. (5) (Established maturity level).	No recommendation	Through a warrant, subpoenas, and court orders in the USA (Established maturity level). In the EU, it depends on the country since they have different approaches.
Are national intelligence services cooperating and exchanging information with foreign services?	There is no explicit law or regulation related to this (Start-up maturity level).	There is a need to explicitly clarify the circumstances under which intelligence services can cooperate with foreign services.	In the USA, they cooperate with Australia, Canada, New Zealand, and the UK. Most of the EU countries cooperate with each other (Established maturity level).
Are data subjects notified of surveillance by intelligence services?	There is no explicit law or regulation related to this (Start-up maturity level).	There is a need to explicitly clarify when and how subjects need to be notified of surveillance by intelligence services.	The answer is "No" for the USA and most of the EU countries except for Finland, Germany, and Portugal (Formative maturity level).
Do data subjects have a right to court review of surveillance measures taken by intelligence services?	There is no explicit law or regulation related to this (Start-up maturity level).	There is a need to explicitly clarify when and how data subjects have a right to court review of surveillance measures taken by intelligence services.	The answer is "Yes" for the USA and most of the EU countries except for Luxembourg, Hungary, Czech Republic, Spain, and Italy (Established maturity level).
Are other governmental bodies (Ministry, Parliamentary Committee, etc.) notified of (individual) surveillance measures taken by intelligence services?	There is no explicit law or regulation related to this (Start-up maturity level).	There is a need to explicitly clarify when and how governmental bodies such as the Ministry, Parliamentary Committee, etc., are notified of (individual) surveillance measures taken by intelligence services.	The answer is "Yes" for the USA and most of the EU countries except for France, Hungary, Italy, Ireland, and Spain (Established maturity level).
Do law enforcement authorities need court orders to intercept communications?	It is possible to submit a request to the general prosecutor according to Article 72, second paragraph of the Federal Criminal Procedure Code (Formative maturity level).	A review of this process needs to be conducted to make it more adaptive to new technologies and circumstances.	The answer is "Yes" for the USA and most of the EU countries except for Ireland (Established maturity level).
How can law enforcement authorities compel companies to provide access to data?	There is no explicit law or regulation related to this (Start-up maturity level).	There is a need to specify the way law enforcement authorities can compel companies to provide access to data.	Through a warrant, subpoenas, and court orders in the USA. In the EU, it needs a court order, but not in Austria (Established maturity level).
Can and do companies challenge orders to provide personal data to law enforcement authorities?	There is no explicit law or regulation related to this (Start-up maturity level).	There is a need to specify the cases when a company can challenge such orders.	The answer is "Yes" for the USA and most of the EU countries except for Italy and the Czech Republic (Established maturity level).

Table 2. List of questions (Part 2)

Questions	*Current situation in the UAE*	*Recommendations*	*Current situation in the USA and the EU*
What privacy rights do individuals have against government agencies and companies if companies share personal data with the government?	There is no explicit law or regulation related to this (Start-up maturity level).	The right of an individual against sharing his/her private data needs to be specified.	In the USA, there are two cases (Baker & McKenzie, 2017): 1) *Against the government via:* 4th & 14th Amendment, Privacy Rights Act of 1974, federal and state electronic communications privacy protections, state constitutional protections, liability, and damages. 2) *Against companies via:* Electronic communications privacy protections, contractual rights. In the EU, member countries follow different laws and policies (Established maturity level).
Are companies liable to data subjects if they disclose data to the government without sufficient legal bases?	According to Article 31 of the UAE Constitution 1971, and its amendments, the privacy of the individual is protected and institutions and companies are responsible for protecting the data of customers and individuals (Established maturity level).	There is no specific article that regulates the sharing of individual private data with the government. Therefore, there is a need to specifically include this in the constitution.	Generally, "Yes" (Established maturity level).
Are data subjects notified if law enforcement accesses their data?	There is no explicit law or regulation related to this (Start-up maturity level).	There is a need to clarify this issue and specify the cases when a subject is notified if law enforcement parties access his/her data and when this notification is not offered.	In the USA and the EU, the answer is "Yes" in most cases. France, Italy, Hungary, Norway, Ireland, and Luxembourg are exceptions (Established maturity level).

6. CONCLUSION

In this paper, we have presented a review and comparison of the surveillance activities that can be conducted by different agents such as intelligent services, law enforcement parties, governments, and companies against individuals and groups in the USA, the EU, and the UAE. We have highlighted the amendments that have been adopted to improve laws in each of these countries, the need for further improvement, and strengths and weaknesses in each. Recommendations have been given in order to help security experts to cooperate with legislators in order to rectify shortcomings and improve the acts adopted in their respected states.

We think that such a comparison can help system developers find an easier way to accommodate the differences in security measures that they have to tackle and incorporate with they are serving customers in these countries and especially in the UAE. A legal framework has been proposed to highlight the context and basis for conducted comparison and the given recommendations. This framework can help researchers as the baseline for future research that is related to surveillance and privacy.

The recommendations given in this paper as answers to eleven questions related to surveillance and privacy can be viewed as a compressive review of the UAE acts and laws in relevance to the focus of this paper. However, these recommendations are associated with the limitations related to the availability of information from various resources that the authors were able to obtain. These recommendations show that for most of the questions the maturity level of laws and acts are still at the Start-up level.

REFERENCES

1. Abokhodair, N., Abbar, S., Vieweg, S., & Mejova, Y. (2017). Privacy and social media use in the Arabian Gulf: Saudi Arabian & Qatari traditional values in the digital world. *The Journal of Web Science, 3*. https://doi.org/10.34962/jws-38
2. Adams, P. C. (2020). Agreeing to surveillance: Digital news privacy policies. *Journalism & Mass Communication Quarterly, 97*(4), 868–889. https://doi.org/10.1177/1077699020934197
3. American Civil Liberties Union (ACLU). (n.d.). *The Foreign Intelligence Surveillance Act — News and resources*. Retrieved from https://www.aclu.org/other/foreign-intelligence-surveillance-act-news-and-resources
4. Baker & McKenzie. (2017). *Global surveillance law comparison guide 2017*. Retrieved from https://tmt.bakermckenzie.com/en/thought-leadership/2017-surveillance-law-comparison-guide
5. Bazan, E. B. (2007). *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*. Retrieved from https://www.everycrsreport.com/reports/RL30465.html
6. Braga, M. (2014, August 6). Sticky data: Why even 'anonymized' information can still identify you. *The Globe and Mail*. Retrieved from https://www.theglobeandmail.com/technology/digital-culture/sticky-data-why-even-anonymized-information-can-still-identify-you/article19918717/

7. Chen, H., Beaudoin, C. E., & Hong, T. (2016). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism & Mass Communication Quarterly, 93*(2), 409–429. https://doi.org/10.1177/1077699016640224
8. Dubai Electronic Security Center (DESC). (2017). *Dubai cyber security strategy: Establishing Dubai as a global leader in innovation, safety and security*. Retrieved from https://www.desc.gov.ae/app/uploads/2020/05/CSS_Eng.pdf
9. European Union (EU). (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
10. Federal Decree-Law No. (5) of 2012. Retrieved from http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf
11. Goldberg, S., Johnson, G., & Shriver, S. (2019). *Regulating privacy online: The early impact of the GDPR on European web traffic & e-commerce outcomes*. Retrieved from https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2019/jul/cs2019_0220.pdf
12. K.N.C. (2019, December 13). Surveillance is a fact of life, so make privacy a human right. *The Economist*. Retrieved from https://www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right
13. Li, Y., Chen, F., Li, T.J.-J., Guo, Y., Huang, G., Frederikson, M.,…Hong, J. I. (2017). PirvacyStreams: Enabling transparency in personal data processing for mobile apps. *The ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 1*(3), 1–26. https://doi.org/10.1145/3130941
14. Open Institute of Information. (n.d.-a). *Electronic surveillance*. Retrieved from https://www.law.cornell.edu/wex/electronic_surveillance#footnote1_67q5rpe
15. Open Institute of Information. (n.d.-b). *Fourth amendment of the US constitution*. Retrieved from https://www.law.cornell.edu/wex/fourth_amendment
16. Rachovitsa, A. (2017). Engineering and lawyering privacy by design: Understanding online privacy both as a technical and an international human rights issue. *International Journal of Law and Information Technology, 24*(4), 374–399. https://doi.org/10.1093/ijlit/eaw012
17. The Global Cyber Security Capacity Centre. (2016). *Cybersecurity capacity maturity model for nations (CMM)* (Revised ed.). Retrieved from https://cybilportal.org/wp-content/uploads/2020/05/CMM-revised-edition_09022017_1.pdf
18. U. S. Department of Justice. (n.d.). *1077: Electronic surveillance*. Retrieved from https://www.justice.gov/archives/jm/criminal-resource-manual-1077-electronic-surveillance
19. Wilkinson, D., & Gibson, B. (2020, June 2). *An introduction to DIFC Data Protection Law 2020*. Retrieved from https://www.lexology.com/library/detail.aspx?g=d3717a08-41ed-4de5-9a95-2249f18d6b41
20. Zalnieriute, M. (2015). An international constitutional moment for data privacy in the times of mass-surveillance. *International Journal of Law and Information Technology, 23*(2), 99–133. https://doi.org/10.1093/ijlit/eav005