AJEE
ACCESS TO JUSTICE IN EASTERN EUROPE
Peer-reviewed Journal

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Special Issue, the Second GPDRL College of Law International Conference on Legal, Socio-economic Issues and Sustainability

Research Article

BUSINESS ETHICS IN E-COMMERCE – LEGAL CHALLENGES AND OPPORTUNITIES

Zaki Mahmed Channak[1], Abdulkader Alkhateeb[2], Elham Saleh[3], Hanadi Aldeeb[4], Sayed Alsharif[5]

Submitted on 12 Feb 2023 / Revised 10 Mar 2023 / Approved **13 Apr 2023**
Published online: **9 May 2023** / Last published: **17 Jun 2023**

1 PhD in Law, associate professor at College of Law, Prince Sultan University, Al-Riyadh, Saudi Arabia, zchannak@psu.edu.sa https://orcid.org/0009-0009-7872-4678
Corresponding author, responsible for project administration, methodology, formal analysis, writing and research. **Competing interests:** No competing interests were declared by the authors. **Disclaimer:** The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organizations.
Translation: The content of this article was translated with the participation of third parties under the authors' supervision. **Funding:** The authors would like to thank Prince Sultan University for supporting this publication. Special acknowledgement is given to the Governance and Policy Design Research Lab (GPDRL) at Prince Sultan University for their academic support to conduct this research and publish it in a reputable journal.
Guest Editors of the Special Issue: Dr. Mohammed Albakjaji, Prince Sultan University, and Dr. Maya Khater, Al Yamamah University, Saudi Arabia.
Managing editor – Dr. Yuliia Baklazhenko. **English Editor** – Dr. Sarah White.

How to cite: Zaki Mahmed Channak, Abdulkader Alkhateeb, Elham Saleh, Hanadi Aldeeb, Sayed Alsharif, 'Business Ethics in E-Commerce – Legal Challenges and Opportunities' 2023 Special Issue Access to Justice in Eastern Europe 101-116. https://doi.org/10.33327/AJEE-18-6S007

2 PhD in Law, Professor at College of Law, Prince Sultan University, Al-Riyadh, Saudi Arabia khateeb@psu.edu.sa https://orcid.org/0009-0008-4864-627X **Co-author**, responsible for methodology, formal analysis, writing and research.

3 PhD in Law, assistant Professor at College of Law, Prince Sultan University, Al-Riyadh, Saudi Arabia Esaleh@psu.edu.sa https://orcid.org/0000-0002-6085-5647 **Co-author**, responsible for writing and research.

4 Lecturer at College of Law, Prince Sultan University, Al-Riyadh, Saudi Arabia hdeeb@psu.edu.sa https://orcid.org/0009-0007-6909-5545 **Co-author**, responsible for Software, Data curation, writing and research.

5 PhD in law, assistant Professor at Prince Sultan University, Al-Riyadh, Saudi Arabia salsherif@psu.edu.sa https://orcid.org/0009-0008-8917-4723 **Co-author**, responsible for conceptualization, writing and research.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Keywords: Ethical issues; challenges; e-commerce; data protection; legal framework; KSA.

ABSTRACT

Background: *This paper deals with the ethical limitations of e-commerce. The aim is to discover areas where the protection is not granted as users would expect and to make proposals for improvement. The authors will begin the paper by proposing the market of e-commerce and how it is directly linked to society's daily life. The method adopted for the legal perspective is case studies, where the Kingdom of Saudi Arabia's (KSA) legal context will be explored. In the end, the paper will answer two main questions: What are the ethical challenges facing the issue of data protection in electronic commerce? What are essential legal frameworks that regulate the subject of data protection in Saudi Arabia?*

Methods: *The normative method is applied to identify the main legislations used in e-commerce and data protection, especially regarding big data regulations. A case study analysis is also used where KSA legislation is investigated.*

Results and Conclusions: *The authors saw that e-commerce is an insecure place to protect customer data. This data is stored electronically, so it is very easy to steal it in addition to the use of this data by companies without the permission of the customer. Research proves that laws are unable to keep pace with technological developments and are unable to provide effective protection for data stored in the cloud.*

1 INTRODUCTION

This paper deals with the ethical limitations of e-commerce. The authors start from the premise of the growing market of e-commerce, which directly links elements of society in our day-to-day life, as the world has become a digital realm and consumers have adopted e-commerce services as part of their lifestyle. The need to establish clear ethical boundaries for e-commerce is rising with this growth. Users of e-commerce expect businesses to adopt strict business ethics to gain their trust. Still, eventually, there should be a legal regulation in place once this trust is broken. This paper aims to establish the correlation between the ethical concerns of businesses and users to the level of protection by regulatory frameworks. The aim is to discover areas where the protection is not granted as users would expect and to make proposals for improvement. The method adopted for the legal perspective is case studies, where the Kingdom of Saudi Arabia's (KSA) legal context will be explored.

This paper will attempt to answer the following questions:

1) What are the ethical challenges facing the issue of data protection in electronic commerce? What are essential legal frameworks that regulate the issue of data protection in Saudi Arabia?

2) What is the availability of criminal protection for the parties to the relationship in the electronic commercial contract, especially the protection of the electronic consumer?

2 METHODOLOGY

In this paper, the authors will use the normative method to identify the main legislations used in e-commerce and data protection, especially regarding big data regulations. A case study analysis is also used where KSA legislation will be investigated. To validate the data we study, the researchers will compare the KSA legislations with those in countries such as France. Finally, this paper will provide recommendations based on this research finding. This method will also be used to conclude the quality and effectiveness of such legislation. The dogmatic approach is involved here as it is the best way to interpret and explain how the KSA legislations govern the issue of consumers' protection in cross-border e-commerce.

3 E-COMMERCE: ETHICAL PERSPECTIVES

The nature of cyberspace (boundarylessness, timelessness, and statelessness) has created legal challenges in applying privacy protection laws to online activities conducted across national states. These activities have often compromised the confidentiality and security of the personal data of online customers in the area of e-business and e-commerce.

Online activity in general and e-commerce in particular is often debated and have acquired a cross-border dimension when the relevant laws and regulations have become null in disputes. Such activities and transactions occur outside the conventional boundaries of time and space that form the basis of tort laws and governmental authorities. In this regard, Wynn and Katz point out that cyberspace allows asynchronous communication, unlike the synchronous communication that occurs within real-time space, as confirmed by Matusitz:

> The cyberspace put an end to geography. Businesspeople are only a mouse click away from Web users in Vietnam or Guatemala. This also implies the death of the time. So, the era of three-dimensional public sphere may become passé.[6]

Over time, cyberspace, or the Internet, has become a virtual space for global business that relies on storing, storing, and transmitting data. Smart devices and cloud computing underpin this type of business. The business case for cyberspace activity has consistently been advantageous due to its features, such as reducing costs, using resources more efficiently, sharing information, growing customer bases, having unlimited time and space, and accelerating business processes. The most crucial factor for online businesses is the consumer's trust based on the security of online data to guarantee the protection of personal or private information. From an organisational and business perspective, the task of protecting the consumer's privacy seems almost elusive in the organisational behaviour where big companies specialising in processing and trading personal-related information conceive of the consumer's data as a commodity.

In effect, cyberspace has made it easier for businesses to carry out data breaches and consequently violate privacy protection rights according to their customers.[7] Companies have also compromised the privacy of their employees, using the Panopticon phenomenon or the electronic eyes in the workplace to control employees and their performance with the excuse of increasing business productivity. Additionally, such malpractices often claim to enhance the customers' trust and loyalty. Using new digital technology, companies have become more equipped to interfere with the private space and private rights of the individual. For

6 Jonathan Matusitz, 'Intercultural Perspectives on Cyberspace: An Updated Examination' (2014) 24 (7) Journal of Human Behaviour in the Social Environment 713, doi: 10.1080/10911359.2013.849223.

7 Andrew Joint, Edwin Baker and Edward Eccles, 'Hey, You, Get Off of That Cloud?' (2009) 25 (3) Computer Law & Security Review 270, doi: 10.1016/j.clsr.2009.03.001.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

example, using biometric data (e.g., face, fingerprints, eyes, and other body parts) to identify a specific individual could damage individual privacy. In this regard, Alterman[8] argues that using, storing, and processing personal information implies three kinds of concern about privacy. Firstly, an individual's data acquired for one purpose may be retrieved, purchased, or correlated with other data without their consent or agreement. The second concern stems from the legitimate access to the individual's information; this may justify the U.S. Federal Bureau of Investigation's (FBI) reasoning for security purposes. So, this may put individuals under pressure where this access can be utilised in a harmful way. The third concern comes from the traditional threat to privacy, where this information can be stolen by criminals who are eager to take advantage of the loopholes that the new technology includes and to hunt personal information. This can expose individuals to the risk of privacy invasion.[9]

Similarly, customers and their activities can be monitored by commercial companies by using loyalty or point cards from which personal information and buying behaviour can be inferred or retrieved to serve the company's purposes. This practice is often justified as necessary to collect marketing information to enhance the customer's experience and address their needs.[10] Yet, such approaches have put privacy at risk and threatened the security of personal information since businesses could transfer and export consumers' data to and from other countries.[11] This threat has affected people's perceptions of cyberspace activities and caused a sense of mistrust and discomfort when their personal information is processed internationally.[12] Recently, digital privacy has become the most focused topic for all news media after the recent revelation that political analysis firm Cambridge Analytica improperly accessed the data of 50 million Facebook accounts.[13] Of course, the scandal has triggered a published apology from Facebook CEO Mark Zuckerberg, admitting that: 'This was a breach of trust and I'm sorry we didn't do more at the time, I promise to do better for you'.[14] The incident has led to severe consequences, such as numerous lawsuits against Facebook, governmental inquiries, a Delete Facebook user boycott campaign, and a sharp drop in share price that has erased nearly $50 billion of the company's market capital.[15] For example, the Federal Trade Commission (FTC) has announced that it is investigating the company's data practices, stating: 'The FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices'.[16]

The investigation examines whether Facebook violated a consent decree the company signed with the FTC agency in 2011. The decree required that Facebook notify users and receive explicit permission before sharing personal data beyond their specified privacy settings.

8 Anton Alterman, '"A Piece of Yourself": Ethical Issues in Biometric Identification' (2003) 5 (3) Ethics and Information Technology 139, doi: 10.1023/B:ETIN.0000006918.22060.1f.

9 Zeynep Tufekci, 'Facebook: The Privatization of our Privates and Life in the Company Town' (*Technosociology: Our Tools, Ourselves*, 14 May 2010) <http://technosociology.org/?p=131> accessed 9 April 2023.

10 Anne Wells Branscomb, *Who Owns Information?: From Privacy to Public Access* (Basic Books 1994).

11 Nancy J King and VT Raja, 'Protecting the Privacy and Security of Sensitive Customer Data in the Cloud' (2012) 28 (3) Computer Law & Security Review 308, doi: 10.1016/j.clsr.2012.03.003.

12 Jan Henrik Ziegeldorf, Oscar Garcia Morchon and Klaus Wehrle, 'Privacy in the Internet of Things: Threats and Challenges' (2014) 7 (12) Security and Communication Networks 2728, doi: 10.1002/sec.795.

13 'Cambridge Analytica: Facebook Data-Harvest Firm to Shut' (BBC News, 2 May 2018) <https://www.bbc.com/news/business-43983958> accessed 9 April 2023.

14 Colin Lecher, 'California Just Passed One of the Toughest Data Privacy Laws in the Country' (The Verge, 28, Jun 2018) <https://www.theverge.com/2018/6/28/17509720/california-consumer-privacy-act-legislation-law-vote> accessed 9 April 2023.

15 Cambridge Analytica (n 13).

16 Peter Kaplan, 'Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices' (*Federal Trade Commission*, 26 March 2018) <https://www.ftc.gov/news-events/news/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection-regarding-reported-concerns-about-facebook> accessed 9 April 2023..

However, the Facebook scandal is the tip of the iceberg, as many other digital companies, such as Google, consistently gather valuable information about online users while surfing the web. Hence, it can be confirmed that there is a great deal of mistrust and uncertainty regarding the depth and breadth of the data that online firms collect for targeted advertising. For instance, in addition to personal information, they collect behavioural information such as web browsing history, search queries, and day-to-day movements in the real world to create individual profiles of online users. However, the most problematic is understanding the concept of privacy within the sphere of digital technology and cyberspace.

Target is just one example of privacy information becoming a significant right that needs serious addressing. Other than selling private data, hacking is another threat to privacy protection, and access was gained to the confidential credit and debit card data of as many as 40 million customers and the personal information, such as phone numbers and addresses, of up to 70 million individuals,[17] compromising the trust of customers. This was not the only damage done to Target's business. Target faces multiple class-action lawsuits, a severely damaged reputation, lost customers, and mounting expenses related to remedying the data breach and restoring stakeholder confidence. Similarly, in 2015, the U.S. Office of Personnel Management was a target of a hacker who stole the information of more than 22 million job applicants and current employees from this office. Hull has claimed that the average number of data breaches continues to increase, and the average cost per breach is 4 million USD.[18] These costs, in most cases, lead to loss of business due to the loss of consumer trust in the wake of a breach. Again, according to the Ponemon Institute,[19] the cost that a company victim incurs ranges from direct cost to indirect cost or loss, such as the impact of the data breach on the company's reputation and expenses of detection and discovery, escalation, notification, and finally, ex-post responses.

In general, e-companies should follow two ethical practices when conducting online commerce:

- Credibility, which means that e-commerce practitioners should avoid deception. In some cases, hackers design fake websites which mimic the original sites in order to deceive consumers and obtain consumers' credit card numbers or personal information about them.
- Honesty, which means that e-commerce practitioners avoid piracy on the Internet and any kind of violation of electronic intellectual property rights.

The challenging aspect of digital technology has become more aggressive with the introduction of 'cloud computing', where the individuals' information and customers' databases are installed on various servers located across geographical boundaries with different jurisdictions and accessed by everyone capable of doing so and from anywhere in the world with no temporal boundaries.[20] Thus, in choosing cloud computing, business companies may store their customers' information on servers and computer systems that they do not own. Hence, they have no control whatsoever over such servers and systems.[21]

17 Lecher (n 14).

18 B Hull, 'Recent Survey Shows Cost of a Breach has Climbed to $158 Per Record' (*Acuntix*, 4 July 2016) <https://www.acunetix.com/blog/articles/recent-survey-shows-cost-breach-climbed-158-per-record> accessed 9 April 2023.

19 'Total Annualized Cost of Cyber-Crime Targeting US Companies in 2014 and 2015' (Statista, 14 October 2015) <https://www.statista.com/statistics/193444/financial-damage-caused-by-cyber-attacks-in-the-us> accessed 9 April 2023.

20 Mohamad Albakjaji et al, 'The Legal Dilemma in Governing the Privacy Right of E-Commerce Users: Evidence from the USA Context' (2020) 11 (4) International Journal of Service Science, Management, Engineering, and Technology 166, doi: 10.4018/IJSSMET.2020100110.

21 Jawahitha Sarabdeen, Gwendolyn Rodrigues and Sreejith Balasubramanian, 'E-Government users' privacy and security concerns and availability of laws in Dubai' (2014) 28 (3) International Review of Law, Computers and Technology 261, doi: 10.1080/13600869.2014.904450.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

This can facilitate the transfer and selling of customers' personal information to other businesses worldwide by the owners of cloud servers. It should be remembered here that the degree of data protection varies from one firm to another and from one country to another as well.[22] Also, individuals do not have the ability to protect the information that is stored in the company system; instead, they have to rely on the protection that the company offers. Unfortunately, the most vulnerable industries that suffer from data breaches are healthcare (31 million records were stolen in 2017) and financial organisations due to the sensitive data stored in their digital system. The WannaCry worldwide cyberattack in May 2017 is a good example. The NHS online systems in the U.K. were paralysed when their stored data was encrypted, and a ransom was demanded to activate and retrieve the data again. This can affect consumer trust, where the data breach will diminish the confidence of current and future customers.[23] Thus, according to Gemalto, criminals shifted from attacking customers' credit cards to attacking and hacking personal information and identity theft,[24] which are very expensive and hard to remedy. For example, in 2016, Yahoo was a victim of a data breach where hackers stole user information from at least 1 billion accounts.[25] Again, the Ponemon Institute[26] has reported that the nature of organisation activities and their locations are the main factors that may determine the possibility of this data breach, with an average of 25.6 % probability. As far as the healthcare industry, Mandian[27] claims that the problem is not spending money to protect personal data or the medical report from leakage but the incorrect policies that are adopted to protect against a threat that may have a catastrophic impact on the business model. So, this industry needs to change its strategies and priorities from treating the breach effect to adopting the proper prevention control. The unfortunate problem is that these companies are spending all their security money to focus on the leakage of personal and medical records. However, they are still implementing the wrong controls to protect against a threat that impacts their entire business model.

4 BUSINESS ETHICS OF E-COMMERCE

From the perspective of businesses, the ethical considerations of e-commerce cannot be seen simply as limitations of their autonomy. They are an integral part of the business policy and strategy. There are several important reasons why a business would firmly integrate ethics into its e-commerce: building the trust of consumers and maintaining a good relationship with the consumers, which impacts consumers' intentions to purchase[28]

Four main principles guide the ethics of the e-commerce provider and user: responsibility and accountability, on the one hand, as business concepts of accepting duties; obligations and costs of the decisions made and determining the accountable persons within the organisation; and liability and due process, a legal concept determining the possibility of

22 Albakjaji et al (n 20).

23 Total Annualized Cost of Cyber-Crime (n 19).

24 'Gemalto Releases Findings of 2015 Breach Level Index' (*Thales*, 23 Febrary 2016) <https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/gemalto-releases-findings-of-2015-breach-level-index> accessed 9 April 2023.

25 Total Annualized Cost of Cyber-Crime (n 19).

26 Ponemon Institute, 2017 *Cost of Data Breach Study: Global Overview* (Ponemon Institute LLC 2017).

27 *Mandiant M-Trends 2018 Report* (FireEye Inc 2018) 1-28.

28 Zhi Yang, Quang Van Ngo and Chung Xuan Thi Nguyen, 'Ethics of Retailers and Consumer Behavior in E-Commerce: Context of Developing Country with Roles of Trust and Commitment' (2020) 11 (1) International Journal of Asian Business and Information Management 107, doi: 10.4018/IJABIM.2020010107.

remedies in case of breach of contract; and a complete understanding of both society and business on how to ensure due process in achieving these rights[29]

The advent of e-commerce has created new opportunities for new businesses to emerge, such as selling digital products (videos, music, games). In addition, using the Internet for commercial purposes with the emerging mobile commerce devices and social commerce has helped companies extend their business and expand their activities. Notably, in populous countries like China and India, which have a high share of online B2C sales in Asia, for instance, the Pacific region, where it reached $1,057 billion, exceeding the United States in second place with $644 billion.[30] The Internet has also enabled new commercial communication methods based on smartphones and social networks that have powered e-commerce activity. Thanks to these tools, the number of online buyers has increased significantly. Online shoppers are expected to grow from 1.66 billion global digital shoppers in 2016 to around 2.14 billion in 2021.[31]

The importance of e-commerce as a convenient way to sell or buy items is always a source of concern to users and customers. However, conducting e-commerce activities is not always safe. One of these concerns is privacy. Currently, customers are concerned about providing their personal information online when they perceive that their personal information is easy prey for hackers roaming the cyber world. The privacy concern does not come from a vacuum; instead, many examples of privacy breaches, hackers, data thefts, and data misuse have raised customers' concerns and made them feel that e-commerce is unsafe. However, it is necessary for their lives.[32]

As a global network, the Internet enables people to communicate and conduct activities across geographical borders) and across different time zones.[33] In this regard, Wynn and Katz argued that cyberspace has enabled asynchronous communication, distinguished from the synchronous communication that occurs inside the real time-space. Accordingly, the physical world has been gradually replaced by the new technology-based virtual world, as confirmed by Matusitz.[34] Based on an environment densely populated with intelligent things, data acquisition has become easily facilitated and compromised,[35] especially in cloud-computing-enabled industries such as e-commerce, where consumers' data is stored and processed for commercial and other purposes.[36] The cloud industry allows businesses to transfer and share customers' data internationally.[37]

These businesses need to build consumers; trust by making their data private and secure to increase their revenue. This task seemed almost elusive in the light of the organisational behaviour where big businesses specialising in processing and trading personal information conceive of this information as a commodity. Also, the recent data breaches involving sensitive data are good evidence that the Internet still exposes consumers to privacy and

29 Khanh Nguyen, 'Business Ethics in E-commerce' (thesis abstract, Seinäjoki University of Applied Sciences, School of Business and Culture 2016) 31.

30 Total Annualized Cost of Cyber-Crime (n 19).

31 Yang, Ngo and Nguyen (n 28).

32 Chris McGuffin and Paul Mitchell, 'On Domains: Cyber and the Practice of Warfare' (2014) 69 (3) International Journal 394.

33 Eleanor Wynn and James Katz, 'Hyperbole over Cyberspace: Self-Presentation and Social Boundaries in Internet Home Pages and Discourse' (1997) 13 (4) The Information Society 297, doi: 10.1080/019722497129043.

34 Matusitz (n 6).

35 Luigi Atzori, Antonio Iera and Giacomo Morabito, 'The Internet of Things: A Survey' (2010) 54 (15) Computer Networks 2787, doi: 10.1016/j.comnet.2010.05.010.

36 Omer Tene and Jules Polonetsky, 'Privacy in the Age of Big Data: A Time for Big Decisions' (2012) 64 Stanford Law Review Online <https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data> accessed 9 April 2023.

37 Honor Mahony, 'EU Gets to Grips with Cloud Computing' (*EU Observer*, 5 April 2011) <https://euobserver.com/news/32048> accessed 9 April 2023.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

security threats on a global scale.[38] So, the peril that threatens information security is the global online activities that allow businesses to transfer and export consumer data to and from other countries.[39] This can become a significant threat to privacy by raising the risk of hackers or crackers who attack computer systems via Internet connections and cause data manipulation, loss, or theft. This threat has affected people's perception of the new technology and its importance to the extent that people feel uncomfortable when asked to provide their personal information on international platforms.[40] Actual data breaches across the world have justified these privacy concerns.

With the introduction of cloud computing, many companies store the personal information they have collected about their customers on servers that other firms own worldwide. The degree of data protection varies from one firm to another and from one country to another, with no ability for individuals to control their personal information stored on those servers; instead, they must rely on the protection offered by online companies.

It is worth mentioning that governing e-commerce activities significantly protects the user's and customers' privacy. This is closely linked to the power of the relevant regulations and legislations and their flexibility to change in line with e-commerce development and technological implementations. For instance, the absence of proper state regulation and lack of adequate laws allow companies to show signs of severe deviations and variations, which could pose threats and challenges to users' privacy. Thus, governing the e-commerce conducts is essential in securing the user's/customers' privacy and personal information stored online. This comes through establishing a new legal system that provides good management of e-commerce privacy issues that can reduce privacy breaches and threats. In recent years and with the advances of technology, establishing this legal system that should be more flexible to change according to these advances has become more necessary than ever. Also, as e-commerce activities are international conducts, there is a need in today's environment to provide a flexible legal system on the international level to harmonise the efforts made for this purpose.

5 LEGAL ANSWERS TO THE CHALLENGES OF DATA PROTECTION IN E-COMMERCE

Liability and due process of business ethics need to be ensured not just through accountability and responsibility of the business but through adequate legal regulation that ensures these principles.

Most scholars have argued that a lack of e-commerce regulations and the absence of strong national and international laws encourage companies to improve their business model rather than protect personal information as a priority.[41] This has become a national problem, where governments cannot implement their laws on disputed cases resulting from trans-border e-commerce interactions. The international characteristics of e-commerce transactions made it difficult for one state to apply its laws over such transactions. Again, on the international level, the issue of customers' privacy is not well protected or governed as there is no international consensus on the need for laws that regulate this issue. Different countries adopt different laws and approaches, and this makes it difficult to govern this issue globally.[42]

38 Joint, Baker and Eccles (n 7).

39 King and Raja (n 11).

40 Ziegeldorf, Morchon and Wehrle (n 12).

41 Daniel Castro and Alan McQuinn, 'Cross-Border Data Flows Enable Growth in All Industries' (*Information Technology & Innovation Foundation*, 24 February 2015) <https://itif.org/publications/2015/02/24/cross-border-data-flows-enable-growth-all-industries> accessed 9 April 2023.

42 Zlatan Meskic et al, 'Transnational Consumer Protection in E-Commerce: Lessons Learned from the European Union and the United States' (2022) 13 (1) International Journal of Service Science, Management, Engineering, and Technology 1.

Activities conducted over the Internet may acquire a cross-border dimension, and potential legal disputes resulting from these activities may lead to a conflict of laws. Although some international laws and rules exist for resolving such disputes, they are not uniform. For instance, online privacy laws differ from country to country, with no proper and sufficient international consensus on the need for laws protecting online users' privacy. Thus, it cannot be said that cyberspace is a lawless zone as the traditional means are still applicable in cyberspace. Still, one may argue that international law has become outdated and invalid for cyber activities for various reasons.[43]

The gap between countries concerning the legal environment needs to be bridged to enhance commerce-privacy protection globally. Therefore, the importance of protecting personal information requires adopting new rules within actual time scope and across boundaries of geographical space. The process is not easily achieved and not without potential challenges to implementers and users of e-commerce. As e-commerce rapidly grows, the challenges of data privacy arise with it. This paper will mainly discuss the ethical issues of privacy and consumer big data protection.

5.1 Data protection

Electronic commerce is directly linked to society in our day-to-day life as the world has become a digital realm, and consumers have adopted e-commerce services as part of their lifestyles. As e-commerce rapidly grows, the challenges of data privacy arise with it.

Collecting data brings new opportunities to modern society and challenges data scientists. Its ethical implications for e-commerce remain empirically under-researched and misunderstood in the era of big data – there has been an explosive growth of information available, and countries have adopted many laws to serve this rapid change. Europe has taken a clear General Data Protection Regulation (GDPR) view on privacy and security, with more people entrusting their data to cloud services and data breaches becoming more common.[44] In Saudi Arabia, the Saudi Personal Data Protection Law and its executive regulations establish the legal foundation for protecting rights concerning the processing of personal data by all entities inside and outside the kingdom. This paper will mainly discuss the ethical issues of privacy and significant consumer data protection.

Consumers may not be aware of the various ways the service collects and analyses information. The electronic apps may collect location and other data, such as chats. In that sense, electronic apps leverage computational behaviour analysis and machine learning to analyse user information such as voice intonations, location data, and screen tips passively or actively collected via apps and wearables, cognitive and behavioural approaches. In ethics, data protection is guaranteed by the Human Rights Act Art. 8(1): Right to privacy: 'Everyone has the right to respect for his private and family life, his home and his correspondence'. Privacy also includes the right to establish an individual's identity and form relationships, such as the right to participate in essential economic, social, cultural, and leisure activities. In certain situations, authorities may need to assist in exercising their right to privacy, including their ability to participate in society. This right granted by the Human Rights Act means that you can prevent the media and others from interfering with your life, so your personal information (official records, photos, letters, diaries, medical records) is safe and not disclosed without permission except in limited circumstances. GDPR in Europe ensures

43 Ben Wolford, 'What is GDPR, the EU's New Data Protection Law?' (GDPR.EU, 2023) <https://gdpr.eu/what-is-gdpr/?cn-reloaded=1> accessed 9 April 2023.

44 ibid.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

data protection by collecting it for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing for public interest archiving, scientific or historical research purposes, or statistical purposes shall be permitted following Art. 89 of the GDPR law.

5.2 Ethical issues of data protection: big data as a challenge

Big data can be defined in many ways, but we can sum it up as follows: large datasets with larger, more diverse, and complex structures that are difficult to store, analyse, and visualise for different processes and results. Extensive data analysis explores large amounts of data to uncover the relationship between hidden patterns.[45]

Big data brings new opportunities to modern society and challenges data scientists. Its ethical implications for e-commerce remain empirically under-researched and ununderstood in the era of big data, which means explosive growth of information available. The movement of such big data will be driven by the fact that vast amounts of very high-dimensional or unstructured data are continuously generated and stored at a much lower cost than before.[46]

Ethics is an essential factor in all respects. However, computing is the development and provision of a required e-commerce system. In other words, information is transmitted and shared electronically through information communication technology. The role of e-commerce telecommunications is vast, making it accessible for users to save the data they need and improve their digital life lifestyle.[47] The right and protection of privacy should be formally granted to an individual, and if respecting the interests of confidentiality is not part of a clear and explicit institutional rule, it is sensitive to privacy interests. Therefore, the distinction between moral and legal rights to privacy depends on whether an individual's interest in confidentiality is significant to their lives and therefore exists. Under Privacy and Data protection, the system will eliminate your data as soon as the purpose of collecting it has expired.[48] However, it may retain such data after collecting it has expired if everything that leads to the specific knowledge of the owner has been removed following the controls specified by the regulations.

Truth is a moral norm that provides the *de facto* accuracy of the information and guides information professionals to the accurate and *de facto* correct handling of personal information. It also expresses ethical virtues such as openness, honesty, and credibility. Freedom is more related to individual freedom of choice and freedom from interference. The Code of Human Rights for Privacy ensures that, as long as there is legal recognition and protection of the right to privacy of an individual, this right should be combined with the freedom of protection from illegal interference by others in an individual's private life. The main ethical issues with data protection and big data are that individuals do not know what happens to their data after it is collected.

Having customer data can benefit electronic apps, but it could lead to misunderstanding, false advertising, poor product quality, fraud, invasion of privacy, abuse of information, and

45 Sam Madden, 'From Databases to Big Data' (2012) 16 (3) IEEE Internet Computing 4, doi: 10.1109/MIC.2012.50.

46 Liu Yahui et al, 'Personal Privacy Protection in the Era of Big Data' (2015) 52 (1) Journal of Computer Research and Development 229, doi: 10.7544/issn1000-1239.2015.20131340.

47 Santosh Kumar Das et al, 'Ethics of E-Commerce in Information and Communications Technologies' (2013) 3 (1-8) International Journal of Advanced Computer Research 122.

48 Saudi Open Data website <https://data.gov.sa/en/PrivacynData> accessed 1 September 2022.

infringement of trust. As commonly acknowledged that the leading reason behind these issues is some retailers' faceless interaction and opportunism.[49]

After discussing the issue of e-commerce and big data, the authors will discuss the examples of new national regulations in comparison with Saudi law, which principles should be followed, and how it should be regulated. The issues of the legal framework and the sanctions for violating the e-commerce and data protection regulations will be covered in the next section.

6 LEGAL FRAMEWORKS FOR VIOLATIONS IN E-COMMERCE

This cyber-crime can be defined as unlawful behaviour in which the criminal – who is assumed to have knowledge of computer technology – uses a computer system or computer network to access data and programs with the aim of copying, altering, deleting, falsifying, sabotaging, rendering invalid, illegally possessing, or distributing them. This crime is characterised by a number of characteristics, such as it does not require violence to be committed, it takes only a relatively short time to commit, it can be committed remotely, it is so difficult to prove such a crime, and the public is unaware of this crime.

The boom of e-commerce during the past few years was not without risks of a criminal nature. In parallel, it was matched by significant growth in electronic crimes, and the e-commerce sector became the preferred sector and fertile ground for cybercriminals due to its breadth and association with other components such as intellectual property, personal data, etc. The studies have revealed that cybercrime rates have increased due to the quarantine in many countries and individuals' reliance on the Internet to secure their needs remotely. The European Police Agency, 'Europol', has announced that the Covid-19 pandemic has contributed to an increase in cybercrime across Europe, especially online fraud,[50] which 'has become the ideal strategy for cybercriminals seeking to sell products that they claim prevent or cure the novel coronavirus'.

The attacks that threaten e-commerce are diverse and expand to risk all its components, such as hacking e-commerce websites, attacking personal data and financial data, electronic payment tools, and third-party intellectual and industrial property rights. In addition, e-commerce has become a fertile field for organised crime and money laundering. In addition, there are violations and crimes that the two parties to an electronic contract may commit. Therefore, it is necessary to strengthen criminal prosecution for e-commerce and to establish criminal responsibility for all acts that threaten it because the declaration of criminal responsibility is of great importance in enhancing public confidence in the safety and health of e-commerce transactions and because of its significant impact on stimulating and developing the e-commerce market at the local levels and international.[51]

Crimes that threaten electronic commerce are of two types: Crimes that threaten electronic commerce in general and crimes between the parties to an electronic contract.

49 Yang, Ngo and Nguyen (n 28).

50 'Dubai police arrest Instagram "stars" behind Dh1.6bn international online fraud scam' (*Arabnews*, 26 June 2020) <https://www.arabnews.com/node/1695321/middle-east> accessed 9 April 2023.

51 HHA Mtwali, 'Criminal Protection of General Trust in E-Commercial Transactions as per UAE' (2014) 23 (4) Conditional Thought 41.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

6.1 Specific crimes that threaten data in e-commerce

These crimes are wide-ranging, including what threatens commerce, threatening the components of electronic commerce, and multiple laws of their own have regulated them. Their penalties are varied, including deprivation of freedom and financial fines in addition to confiscation; organised crime and money laundering are among the most dangerous, together with access to a merchant's website, e-mail, and components. E-commerce has become the easiest way to commit organised crime and money laundering. Where organised criminal groups conduct their commercial activities over the information network away from the direct control of law enforcement authorities, commercial websites are created on the dark web, and their products are offered under false conditions.

1. Organised crime and money laundering crime in electronic commerce.

Organised criminal groups adopt one of two methods of perpetrating organised crime in the context of e-commerce; either by engaging – using pressure and threats – in the activity of legal e-commerce companies, pumping dirty money into the financial assets of e-commerce companies to purify it and recycle it as clean money (legitimate,)[52] or by illegally practising electronic commerce by creating illegal commercial markets on the Internet, through which counterfeit products are offered,[53] the revenues of which are estimated at approximately 250 billion dollars annually, according to the report of the United Nations Office on Drugs and Crime. In this regard, Europol in Europe arrested a group of people running a market on the dark web as they pumped counterfeit banknotes estimated at 1.3 million euros into an illegal market called the 'Wall Street Market', the second largest electronic market for trade in the dark web.[54]

2. Illegal access to a merchant's websites and infringement of its components.

This type of attack is classified as a cybercrime, especially among the crimes of infringing the information systems of the commercial website and tampering with the data and data of the website. Comparative penal laws provide punishment of illegal entry to the site with imprisonment and a fine or one of them, as in the Saudi cybercrime law (Art. 3, n.3) and the UAE IT Crimes Law 2021 (Art. 2, n.1). The Syrian Information Crime Law of 2022 distinguished between illegal entry, punished by imprisonment and a fine (Art. 12), and overstepping the legitimate entry, penalised with a fine only (Art. 11). If the illegal entry in its various forms leads to damage to the components of the site, or infringement in any way whatsoever, it is considered in the Saudi and UAE laws as an aggravating circumstance for the penalty, incurring both types of imprisonment and a fine, as in Syrian law, which distinguishes between illegal entry and exceeding the limits of legitimate access.

6.2 The crimes of electronic traders

The e-merchant has many obligations, most of which are in the protection of the electronic consumer as the weakest party in the commercial electronic contract. In this regard, the e-merchant must provide adequate data about his store and the service or product he offers; otherwise, he will be subject to criminal liability.

52 Philippe Véry and Bertrand Monnet, 'Comment le crime organisé s'empare des actifs de l'entreprise' (2009) 2 (2) Securite et Strategie 4, doi: 10.3917/sestr.002.0004.

53 ONUDC, *Gros plan sur: Le trafi c illicite de biens contrefaits et la criminalité transnationale organisée* (ONUDC 2013).

54 'Europol Arrests 11 People who Run a Market on the Dark Web' (*Euronews*, 17 December 2019) <https://arabic.euronews.com/my-europe/2019/12/17/europol-arrests-11-people-who-run-a-market-on-the-dark-web> accessed 9 April 2023.

6.2.1 Failure of the e-merchant to fulfil its pre-contractual obligations

To varying degrees, e-commerce laws and consumer protection laws obligate the electronic merchant to provide a large set of pre-contract data to guarantee that the consumer will obtain as much information as possible to enable him to make his decision in the contract. French law is one of the most recent laws in this field, as by decree (Décret n° 2022-424 du 25 mars 2022),[55] which entered into force on 28 May 2022. It expanded the obligations of the electronic merchant stipulated in the Consumer Code (art, L. 111-1 et aux articles L. 111-2 et L. 111-3).

The most important obligations of the electronic merchant in comparative law:

a) Procedures to be taken to conclude the contract and to clarify the contracting steps.

b) Adequacy of data to define the service and product well in terms of its characteristics and type of quality.

c) A statement of the price, including all fees, taxes, or additional amounts related to delivery, if any. If there are discounts on the product, the old and new prices must be clearly displayed.

d) His name or the name of the company, the address of the company's headquarters, the entity with which he is registered, the country in which he is registered, his phone number and e-mail address, as well as the data related to his deputy, if any.

e) The available electronic means of communication while ensuring that the consumer is allowed to record all written communications exchanged with the merchant, as well as the cost of using remote communication technology to conclude the contract when this cost is calculated on a basis other than the basic tariff.

f) Payment methods and payment terms that can be included in the contract.

g) Data relating to guarantees and their duration.

Comparative laws punish breaching these duties with a fine and some administrative penalties. In Art. 18, the Saudi E-Commerce Law punishes the breach of obligations stipulated in the same law with the following sentences: A- Warning. B- A fine not exceeding (1,000,000) one million riyals. C- Temporarily or permanently suspending the practice of electronic commerce. D- Blocking the electronic store – in coordination with the competent authority – partially or entirely, temporarily or permanently. On the other hand, the penalty is an administrative fine in French consumption law, which does not exceed 3,000 euros for a natural person and 15,000 euros for a legal person. UAE law considers every condition that exempts the merchant from any obligations stipulated in the Consumer Protection Law as null (Art. 21).

6.2.2 The crime of deceiving and misleading the consumer.

Due to the specificity of remote contracting, which depends primarily on advertising and publicity through electronic media, comparative laws in electronic commerce have prohibited the electronic merchant (service provider) from including the electronic advertisement as an offer, statement, false claim, or phrases that may lead directly or indirectly to Deceive or mislead the consumer, such as exaggerating the description of the product inconsistent with

55 Décret n°2022-424 du 25 mars 2022 'Relatif aux obligations d'information précontractuelle et contractuelle des consommateurs et au droit de rétractation' <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045410578> accessed 9 April 2023.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

reality or placing any indication or indication of the application of a quality management system, or the advertisement containing a phrase that deludes the consumer that the product is about to run out, or a logo or trademark that the service provider does not have the right to use, or a counterfeit mark to induce the consumer to contract.

The French consumption law punishes misleading advertising with two years in prison and a fine of 30,000 euros (Art. L132-2 Modified par LOI n°2021-1104 du August 22 2021). If the misleading advertisements result in a decade or more, the penalty shall be three years in prison (Art. L132-2-1 Creation LOI n°2022-1158 du August 16 2022 – Art. 20). In the event that this crime is committed by an organised gang, the penalty shall be seven years imprisonment, (Art. L132-2-2 Creation LOI n°2022-1158 du August 16 2022 – Art. 20).

In Art. 18, the Saudi Electronic Commerce Law punishes merely misleading advertisements with a financial fine not exceeding (1,000,000) million riyals and some administrative measures. However, if the misleading advertisement contains the elements of the material element of the crime of fraud, such that the misleading advertisement includes, for example, lies or deception, or if it would delude in any way of fraud that the opportunity is suitable for contracting and the deal is undoubtedly profitable, what prompted the consumer to contract, then the one responsible for the advertisement shall be punished The misleader shall be liable for the fraud crime stipulated in Art. 1 of the Anti-Financial Fraud and Breach of Trust Law. The misleader shall get imprisonment for a period not exceeding (seven) years and a fine not exceeding (five) million riyals or one of these penalties. This penalty does not prevent the addition of another penalty mentioned in Art. 18 of the Electronic Commerce Law in a manner that does not conflict with imprisonment and fines.

6.2.3 The abuse of electronic consumer personal data

The completion of e-commerce transactions entails recording the personal data of the electronic consumer and keeping it within the information system of the electronic trader, who must respect this data and not be allowed to touch it in any way. Otherwise, he will expose himself to criminal responsibility.

The electronic merchant may not keep the personal data of the consumer or his electronic communications except for the period required by the nature of dealing in electronic commerce, and he shall be responsible for maintaining this information that is in his custody or under the control of the parties he deals with or with their agents. He must destroy it once its purpose has expired (Art. 18 of the Saudi Personal Data Protection Law, criminal law fr. art. 226-20)

The service provider may not use the consumer's data or electronic communications for unauthorised or permitted purposes or disclose it to a third party, with or without payment, except with the consent of the consumer to whom the personal data relates (Art. 5 of the Saudi E-Commerce Law, criminal law fr. art. 226-16 and next).

Saudi law punishes compromising the consumers' data with imprisonment for a period not exceeding (two years) and a fine not exceeding (three million) riyals or one of these two penalties. The Saudi legislator requires a special criminal intent to harm the data owner or achieve a personal benefit to apply this penalty (Art. 35 of the Personal Data Protection Act), while the liability in French law is five years imprisonment and a fine of 300,000 euros. There are special penalties for a legal person.

7 CONCLUSIONS

In the end, the world has become a digital empire, and consumers have embraced e-commerce services as part of their lifestyle; e-commerce is directly connected to society in our daily lives. As e-commerce multiplies, so does the data protection challenge; as such, it is necessary for countries to promote awareness of the moral and legal rights related to the processing of personal data. In particular, there is a necessity to identify a specific age for electronic consumers, as most laws do not set an age limit. The main ethical challenges are collecting data from individuals and needing to disclose how the electronic apps handle the data. It is necessary to strengthen international and regional cooperation to allocate special laws to protect personal data from abuse and hacking and to urge countries to develop their internal security systems similar to the Saudi regulator in the Personal Data Protection Law, its administrative regulations, and the Cybersecurity Law. It should be an obligation for electronic merchants to report any attack on consumer data. One of the significant ethical concerns is advertising based on big data since it might lead to false advertising based on consumer's data and research history, and it would lead to fraud, invasion of privacy, misuse of information, and infringement of trust and that would conflict with the guaranteed right to privacy for individuals. The authors believe in criminalising electronic commerce organised by criminal groups in the Saudi regulator of electronics in line with French law, enhancing international and regional cooperation in organising procedures for prosecuting e-commerce crimes.

REFERENCES

1. Albakjaji M et al, 'The Legal Dilemma in Governing the Privacy Right of E-Commerce Users: Evidence from the USA Context' (2020) 11 (4) International Journal of Service Science, Management, Engineering, and Technology 166, doi: 10.4018/IJSSMET.2020100110.
2. Alterman A, '"A Piece of Yourself": Ethical Issues in Biometric Identification' (2003) 5 (3) Ethics and Information Technology 139, doi: 10.1023/B:ETIN.0000006918.22060.1f.
3. Atzori L, Iera A and Morabito G, 'The Internet of Things: A Survey' (2010) 54 (15) Computer Networks 2787, doi: 10.1016/j.comnet.2010.05.010.
4. Branscomb AW, *Who Owns Information?: From Privacy to Public Access* (Basic Books 1994).
5. Castro D and McQuinn A, 'Cross-Border Data Flows Enable Growth in All Industries' (*Information Technology & Innovation Foundation*, 24 February 2015) <https://itif.org/publications/2015/02/24/cross-border-data-flows-enable-growth-all-industries> accessed 9 April 2023.
6. Chaudhary R and Lucas Mi, 'Privacy Risk Management' (2014) 71 (5) Internal Auditor 37.
7. Das SK et al, 'Ethics of E-Commerce in Information and Communications Technologies' (2013) 3 (1-8) International Journal of Advanced Computer Research 122.
8. Hull B, 'Recent Survey Shows Cost of a Breach has Climbed to $158 Per Record' (*Acuntix*, 4 July 2016) <https://www.acunetix.com/blog/articles/recent-survey-shows-cost-breach-climbed-158-per-record> accessed 9 April 2023.
9. Joint A, Edwin B and Edward E, 'Hey, You, Get Off of That Cloud?' (2009) 25 (3) Computer Law & Security Review 270, doi: 10.1016/j.clsr.2009.03.001.
10. King NJ and Raja VT, 'Protecting the Privacy and Security of Sensitive Customer Data in the Cloud' (2012) 28 (3) Computer Law & Security Review 308, doi: 10.1016/j.clsr.2012.03.003.
11. Madden S, 'From Databases to Big Data' (2012) 16 (3) IEEE Internet Computing 4, doi: 10.1109/MIC.2012.50.
12. Matusitz J, 'Intercultural Perspectives on Cyberspace: An Updated Examination' (2014) 24 (7) Journal of Human Behaviour in the Social Environment 713, doi: 10.1080/10911359.2013.849223.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

13. McGuffin C and Mitchell P, 'On Domains: Cyber and the Practice of Warfare' (2014) 69 (3) International Journal 394.
14. Meskic Z et al, 'Transnational Consumer Protection in E-Commerce: Lessons Learned from the European Union and the United States' (2022) 13 (1) International Journal of Service Science, Management, Engineering, and Technology 1.
15. Mtwali HHA, 'Criminal Protection of General Trust in E-Commercial Transactions as per UAE' (2014) 23 (4) Conditional Thought 41.
16. Nguyen K, 'Business Ethics in E-commerce' (thesis abstract, Seinäjoki University of Applied Sciences, School of Business and Culture 2016).
17. Sarabdeen J, Rodrigues G and Balasubramanian S, 'E-Government users' privacy and security concerns and availability of laws in Dubai' (2014) 28 (3) International Review of Law, Computers and Technology 261, doi: 10.1080/13600869.2014.904450.
18. Tene O and Polonetsky J, 'Privacy in the Age of Big Data: A Time for Big Decisions' (2012) 64 Stanford Law Review Online <https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data> accessed 9 April 2023.
19. Tufekci Z, 'Facebook: The Privatization of our Privates and Life in the Company Town' (*Technosociology: Our Tools, Ourselves*, 14 May 2010) <http://technosociology.org/?p=131> accessed 9 April 2023.
20. Véry P and Monnet B, 'Comment le crime organisé s'empare des actifs de l'entreprise' (2009) 2 (2) Securite et Strategie 4, doi: 10.3917/sestr.002.0004.
21. Wolford B, 'What is GDPR, the EU's New Data Protection Law?' (*GDPR.EU*, 2023) <https://gdpr.eu/what-is-gdpr/?cn-reloaded=1> accessed 9 April 2023.
22. Wynn E and Katz J, 'Hyperbole over Cyberspace: Self-Presentation and Social Boundaries in Internet Home Pages and Discourse' (1997) 13 (4) The Information Society 297, doi: 10.1080/019722497129043.
23. Yahui L et al, 'Personal Privacy Protection in the Era of Big Data' (2015) 52 (1) Journal of Computer Research and Development 229, doi: 10.7544/issn1000-1239.2015.20131340.
24. Yang Z, Ngo QV and Nguyen CXT, 'Ethics of Retailers and Consumer Behavior in E-Commerce: Context of Developing Country with Roles of Trust and Commitment' (2020) 11 (1) International Journal of Asian Business and Information Management 107, doi: 10.4018/IJABIM.2020010107.
25. Ziegeldorf JH, Morchon OG and Wehrle K, 'Privacy in the Internet of Things: Threats and Challenges' (2014) 7 (12) Security and Communication Networks 2728, doi: 10.1002/sec.795.