Journal of the Arab American University مجلة الجامعة العربية الامريكية للبحوث

Volume 8 | Issue 1 Article 1

Online Privacy Challenges and their Forensic Solutions

Bandr Fakiha
Umm Al-Qura University, Saudi Arabia, bsfakiha@uqu.edu.sa

Online Privacy Challenges and their Forensic Solutions

Cover Page Footnote

Online Privacy Challenges and their Forensic Solutions

Bandr Fakiha

Department of Medical Health Services, Faculty of Health Sciences, Umm Al-Qura University-Saudi Arabia

bsfakiha@uqu.edu.sa

Abstract

In the digital age, internet users are exposed to privacy issues online. Few rarely know when someone else is eavesdropping or about to scam them. Companies, governments, and individual internet users are all vulnerable to security breaches due to the challenges of online privacy ranging from trust and hierarchical control to financial losses. As systems advance, people are optimistic that forensic science will provide long-term interventions that surpass the current solutions, including setting stronger passwords and firewall protection. The future of online privacy is changing, and more practical interventions, such as email, malware, mobile, and network forensics, must be integrated, reducing privacy issues online.

Keywords: Internet of Things (IoT), privacy, security, online, individuals, corporates, challenges, solutions, users.

Introduction

Digitalization comes with a fair share of challenges as well as benefits. The ability to keep safe online is a significant milestone that sometimes requires institutional policies and interventions (Lakshmi & Mohideen, 2013). This discourse aims to analyze how technology can advance communication online while keeping people safe (Atlam et al., 2020). People live in the information age, and they are predisposed to unethical practices that land their data in wrongful hands. For instance, IoT based forensic model ensures "identification, acquisition, analysis, and presentation of potential artifacts of forensic interest," as seen in Amazon Echo (Li et al., 2015). As such, they use the acquired information to recommend songs, command smart devices to internet search. In addition, people spend most of their time on social networking platforms, businesses on their e-commercial sites, while organizations strive to promote customer satisfaction via Zoom and other digital applications (Singh et al., 2018). Often, privacy violations are bound to happen, and entities are seeking long-term solutions for these violations. Moreover, Internet of Things (IoT) integration into various industries requires effective digital forensics in handling the growing cyberattacks (Lutta, et al., 2021). This submission will use a quantitative research methodology to collect data using systematic reviews and experiments. The research method will be experimental. Data analysis through regression methods will assist in the generation of results from mathematical and statistical functions. Generally, maintaining privacy online is every user’s dream, but achieving it remains a nightmare at personal and institutional levels. Ways of improving safety and increasing privacy online must be implemented in every online interaction via forensic solutions, as will be determined.

Questions & Hypothesis

The underlying research question is, how and what are the benefits that forensic solutions offer to organizations, governments and individuals in enhancing privacy online?

What are the limitations of these digital forensic solutions, such as fog nodes in promoting online privacy?

Lastly, in what ways can various stakeholders ensure the effectiveness of these digital forensic solutions?

With the growing rise of online privacy issues (independent variable), digital forensic solutions offer somewhat of a lifeline in mitigation of these privacy issues (dependent variable). This is the underlying hypothesis of the study.

Materials and Methods

This study will involve the identification of themes from systematic reviews. The experimental approach will be a quantitative study and a quasi-experimental design. The sampling method will be stratified to ensure that only articles that meet the criteria are included. Articles will be from credible databases, such as Ebscohost and Google Scholar. The articles will strive to draw a relationship between challenges to online privacy and forensic solutions. Of great significance will be the role of internet users or consumers who spend their time and resources risking their privacy.

This is a non-commercial research process meaning, that the output will be used for informational purposes, but not financial It will apply a quantitative research methodology and experimental studies as the research method. Experimental research is embedded in systematic reviews, unlike other cohort studies, randomized controlled trials, and observational case-control studies (Edmonds & Kennedy, 2019). During experimental studies, researchers introduce the effects of a study after discussing the interventions. Systematic reviews provide the most substantial evidence in research, making them critical for this submission. Also, randomized controlled trials (RCTs) also limit bias but mostly work best in clinical research, such as new drug trials.

In the ongoing controlled experiment, data on the effects of cybercrime on online privacy will be investigated. Of great interest, an analysis of forensic solutions will be aimed at addressing these emerging problems. During the research, numerical data will be sought. In systematic reviews, questions are formulated, and the response is used to develop arguments. This analysis will utilize at least 120 articles to examine the relationships between forensic solutions and online privacy challenges. Through strategic sampling, only highly relevant articles to the study question will remain (Wang & Fan, 1998). In addition, the articles will have to be relevant, and at least 75% will be dated 2014-2021. Most will be peer-reviewed journals and books.

The researcher will concentrate on articles that discuss serious online privacy violation issues and forensic interventions related to the problems. Variables in the study will include internet users, challenges of online privacy, and solutions to the problems, besides the independent and dependent variables, moderator variables. Due to the high numbers of variables, simple regression analysis will be used. For instance, users are the dependent variables because their behaviors are affected by online privacy. Online privacy challenges represent independent variables, while forensic solutions act as moderator variables.

Arguably, most users are online and oblivious of data privacy issues related to their internet searches. Often, when one searches for an item on an e-commercial platform, the chances are that the company would recommend other similar brands. In essence, every time one goes online, chances are that they are selling some part of their private data to an internet service provider or a marketer. These challenges are unchanging, and this explains why they represent the independent variable. Nonetheless, the attitudes of users change when informed about levels of privacy compromised online. As such, they might change their behaviors by putting stronger passwords, creating firewall protection, and even browsing in private windows to avoid exposure to unsolicited parties. Also, entities are known for providing necessary interventions to minimize privacy violations when users are online.

The data extracted from systematic reviews will be analyzed to examine the problems and manipulated to develop solutions. This approach follows the principles of quasi-experimental designs that permit data production, alteration, and measurement to suit the researcher's context (Campbell & Stanley, 2015). Quasi-experimental study designs are effective because they enhance the predictability of outcomes (Reichardt & In Little, 2019). The quantitative methodology will be contextualized by expressing findings in numerical figures. This type of data is often easy to interpret, and the measurements are occasionally grouped (Yuan & Lin, 2006). Price, Jhangiani, and Chiang (2015) believe that the ease of interpretation roots from describing findings using statistics.

Numerical or statistical data records offer high validity and accuracy rates. According to Lakshmi and Mohideen (2013), the study approach draws more links between independent and dependent variables because no quantifiable information can be based on observable assumptions. Researchers must use nominal scales of measurement to determine that online privacy affects users and those interventions are available to reduce the impacts of the problem. Quasi-experimental designs are excellent for this study because they do not have confounding variables (Campbell & Stanley, 2015). In essence, researchers do not have to focus on control groups (Price et al., 2015). Still, mediator variables strongly influence outcomes during natural experiments.

Another interesting bit of the study will be to perform pre-test and post-test experiments. Researchers always plan to implement the intervention in such studies based on how successful the outcome is on the study population (Dhiman, Sen, & Bhardwaj, 2018). During pre-test and pro-tests, certain conditions must be created for the expected outcomes to be realized (Keren, 2014). For instance, the systematic reviews will include populations that have been exposed to online privacy challenges and those that have never experienced it.

Other articles will involve populations that have been exposed to various interventions after experiencing online privacy challenges. The rationale will be to determine the behaviors of the two groups through randomized controlled trials exhibited in various articles.

Results

The research used linear regression analysis, and the variables were grouped into two to establish their relationship. Other regression analyses exist, including non-linear, multiple-linear, and linear (Stanley & Jarrell, 2005). The formula below applies when using linear regression analysis

Y = a + bX + ϵ [X represents the independent variable; Y stands for the dependent variable, “a" refers to the intercept; b means the slope, and ϵ is the residual error]

The study sought to establish the relationship between online privacy and users with the interception of forensic solutions. First, it is important to establish the challenges that arise from online engagement. The patterns and behaviors of the users were recorded before any solutions were implemented, and the produced behavior was monitored. Also, slight errors are common in regression analyses, and this explains the deliberate input of ϵ.

Y (challenges of online privacy) **= a** (solutions) **+ bX** (Slope*users) **+ ϵ ………………** (1)

An important component of the equation is the slope, calculated as m = r(SDy/SDx) (Yuan & Lin, 2006). In this context, a researcher divided delta y by delta x. In the study, 120 articles were chosen. Only 60 articles contained the right themes and met the selection criteria. Forty (40) of the articles were correctly identified, noting the challenges of online privacy without detailing any action plans. The other twenty (20) discussed interventions. Both groups of articles had impacts on users. Since half of the articles were selected, this was as qualified as 50%. The slope is calculated as delta y/delta x (60/20) =3 (2). As such, the linear regression analysis was calculated as 60=20+3*(120/50) +residual error (+/- 0.1) (3).

Based on the summary, challenges of online privacy identified from the 60 articles included:

a. Devices’ proliferation

At least 75% of the 60 articles argued that when people used various devices on their machines, they faced the challenge of managing big data. Digital forensics is vital in the analyses of these data to determine its vulnerabilities, and a task tasked to digital forensic experts (Choi, 2021). The possibility of being compliant with the organizational data protection rules is low. Also, more data means additional responsibilities and confusion (Conti, Dehghantanha, Franke, & Watson, 2018).

Most users fall victim to such problems, but with an intervention, such as data governance, the possibility of making mistakes is reduced. During the regression analysis, 80% of the 20 articles confirmed that data governance is a step in the right direction.

b. Data visibility

Data visibility is a sensitive topic because people can easily hack and access others' information today. The bad culture seems unstoppable, with 85% of the 60 articles reporting that some organizations and individuals have been sabotaged because information landed in the wrong hands. The regression analysis further confirmed that no permanent solution to data privacy exists. Still, anonymization could be observed, and during data synchronization, one must be careful not to leave any traces. In addition, institutions should prioritize the development of a data management strategy and personnel training. Also, 90% of the 20 articles confirmed that developing privacy policies would enhance security and promote privacy.

c. Maintenance costs

Whenever security breaches occur, businesses and individuals spend a fortune to regain data and rebuild their image. According to 70% of the 60 articles and 71% of the 20 articles, a user of online services incurs losses when privacy and security breaches occur. Therefore, individuals and businesses are keen on finding long-term solutions to their problems. If not, they will continue to incur more losses associated with high maintenance costs. The chart below reveals how much businesses and individuals are likely to lose because of privacy and security challenges experienced online.

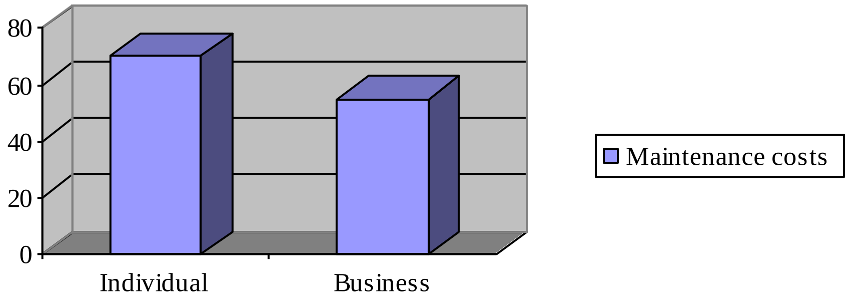

Figure 1: Categories of articles used

Occasionally, maintenance costs increase when operating at individual levels are compared to organizational ones. Globally, digital platforms run to support isolation but enhance communication. Often, when reputational damage occurs to an individual, the possibility of rebuilding the image and recovering the data depends on how much the person is willing to lose.

Companies are better placed due to their excellent backup systems tracing online identities using data infrastructures created since inception (Atlam, et al., 2020). Several other themes emerge from the different peer-reviewed articles, including data sovereignty concerns, the emergence of powerful entities that will control the internet in the future, and trust issues that must be addressed carefully to avoid exposing users to harm.

Discussion

The Internet of Things (IoT) is one of the most popular terms of the digital age. Still, IoT faces significant setbacks in security and privacy concerns (Stoyanova, Nikoloudakis, Panagiotakis, Pallis, & Markakis, 2020). Thus, digital forensics improves on the shortcomings of IoT through a forensic framework providing "distributed computing, decentralization, and transparency of forensic investigation of digital evidence" (Kumar, et al, 2021). Users are often unaware of device monitoring and continue browsing without realizing the danger of sharing information with unwelcome parties. As this happens, there is almost nothing the aggrieved parties can do to resolve the stalemate because security protocols for protecting online clients are almost inexistent. Another huge concern is the challenge of incorrect device updates, which makes a user vulnerable to phishing. Razi, Agha, Chatlani, and Wisniewski (2020) mentioned that such security scares are better addressed by asking users to secure their devices individually. For instance, IoT applications can prevent excessive information leakage to platforms such as the Amazon Web Service - renowned virtual machines (Tawalbeh, Muheidat, Tawalbeh, & Quwaider, 2020). Besides applications, users must always ensure that they are not exposing personal data on social networking platforms. Already, WhatsApp initially sent out a new set of terms and conditions to synch the social media platform with Facebook. The move would cause serious privacy violations, and users were warned to be careful before accepting the terms. This was a security intervention at a personal level, which helped some users to protect their online identities.

Cloud storage is another popular term because it helps several users not to worry about expanding their device capacities. As illustrated in Figure 2, cloud, device sensors, and end-users are interconnected. Therefore, it is almost impossible to keep private life away from the public.

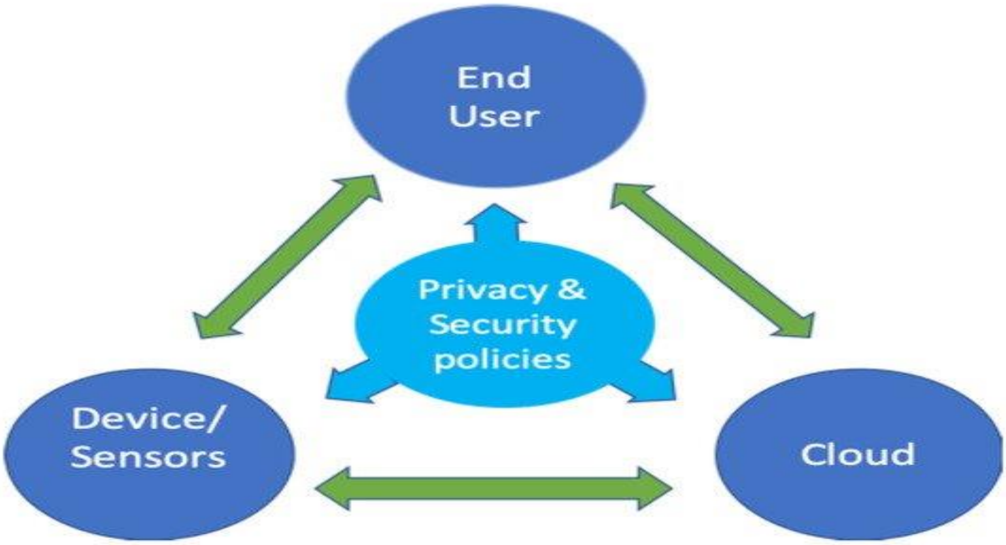

Figure 2: Cloud storage for management of personal data

Consistently, an unsolicited party manages the data. For instance, cloud storage for media and Electronic Health Records for medical data seems like the safest ways of data management for users (Wang et al., 2018). Still, the data is vulnerable to hacking, and no legal interventions exist to protect people against online privacy violations. The argument used by most culprits is that nobody owns the internet. As such, an offender cannot be tried in any country because the privacy violation offense occurs in the cloud or space. Similar concerns are manifested in workplaces when human resources administrators access personal information without contextualizing how their actions violate moral values (Hasan, Chamoli, & Alam, 2020). In essence, people are expected to be custodians of others' information when responsible for electronic data. In workplaces, information that needs to remain a secret must be kept, and severe administrative actions should be taken against managers who violate privacy rights. Also, when companies have central databases, those managing data should not spend time monitoring other people’s information. If not, legal actions should be taken against them. As it is, criminalizing online privacy violations is difficult, and on countless occasions, institutions are equally forced to monitor the activities of offenders to strengthen their cases against them. As a result, the chances of violating privacy ethics increase. Therefore, the concept of online privacy management is complex without legislative or policy interventions.

Privacy is a personal life condition, which affirms the need for exclusion from publicity. Data protection policies vary based on the Acts of Parliament or congressional Acts.

At a regional level, the Guidelines for the Protection of Privacy and Transborder Flow of Personal Data were endorsed by the Economic and Coordination and Development (OECD) for member states (Atlamet al., 2020). While autonomy should be conditional and a product of self-pursuit, some people do not enjoy it. Most of them predispose themselves to the wrong crowds through digital platforms. Eavesdropping, hacking, spying, phishing sabotage privacy, and necessary interventions such as strong passwords and firewall protection should be used to reinforce cybersecurity, alongside forensic solutions (Atlamet al., 2020). After reviewing the results carefully, a recurrent theme is that challenges of online privacy affect communications, the body, information, and possessions. Arguably, digital platform users can unconsciously expose medical or financial information to fraudsters, scams, or enemies. Therefore, personal browsing behavior and information sharing traits should be assessed before opting for stronger passwords or firewall protection. Enacting legislative actions against online privacy violations has proved difficult for many countries. As such, people are encouraged to take personal responsibility to avoid exposing personal data to unsolicited parties.

In a study conducted by Singh, Halgamuge, Ekici, and Jayasekara (2018), the researcher collected information from fifty-eight peer-reviewed articles dated 2007 to 2016. The rationale was to establish the possibility of addressing confidentiality issues associated with big data. The study addressed privacy concerns in various industries, such as robotics, healthcare, finances, social media, web applications, and mobile communications. The researcher had no conclusive argument. Instead, the study recommended that users should wait for futuristic research that gives them a better direction on privacy management for big data. Corporate entities are waiting for solutions to secure data and enhance the privacy of their employees. In comparison, Singh et al. (2018) show limited optimism; Abraham, Saravanan, and Smith (2019) mention that the security threats come from hierarchies that affect the implementation of necessary interventions. For instance, Fog Computing is expected to be safe, yet vulnerabilities surface, giving hackers a chance to access private information. Cisco created Fog Computing as a forensic solution, but online predators still intercepted security controls. Thus, Fog forensics are crucial solutions towards online privacy issues due to fog nodes that reduce “low latency, location awareness, and geographic distribution unsupported features of many IoT applications” (Alzoubi, et al., 2021). This forensic solution is only hindered by the lack of effective legislations. While the most realistic thing to do would be to identify and punish offenders, one would question why the likes of Julian Assange of Wikileaks were freemen for a long time.

In essence, hierarchies continually affect the strategic implementation of security measures, and sometimes the creators of IoT lack control over their products and services. Table 1

Table 1: Forensic solutions and their applications

Forensic Solutions	Applications
Forensic hunting tools, such as YARA	Malicious software identification
Powerful packet capture, such as Observer GigaStor	Packet-level storage and recall
Network forensics, such as Observer GigaFlow	Improve recall in unstructured and structured flow-based data sets
Maltego CE, forensic solution	Conducting investigations online
Cuckoo Sandbox, forensic solution	Elimination of suspicious files
CrowdFMS, emailing forensics	Explication of phishing emails

Conclusion

No outlined solutions exist to comprehensively target online privacy issues arising at individual and corporate levels. Even forensic solutions are limited by certain circumstances, such as the soundness of investigators and the inability to traverse hierarchies when seeking verifiability. Even forensic infrastructures, such as Crime-as-a-service (CaasS) model, have been affected by cyber security issues and sophistication of specific data governance procedures. In essence, since privacy is unconditional, it is difficult for people to assist forensic scientists with specific information in starting investigations and preventing similar problems in the future. Therefore, interventions for online privacy challenges remain at institutional and individual levels.

Recommendations

Forensic scientists should work with military intelligence to generate permanent solutions for the current problems. According to Joshi and Gupta (2019), recurring online privacy issues include scamming and gambling. People are discouraged from sharing personal banking details, but scammers are becoming smarter, and some still steal from unsuspecting individuals. Forensic email, malware, mobile, and network are crucial towards identified weaknesses in systems and databases. However, network and other types of forensics are coupled with several challenges, such as “high storage speed, the requirement of ample storage space, data integrity, data privacy, access to IP address, and location of data extraction” (Qureshi, et al., 2021). These challenges undermine their continued integration. If the military and forensic scientists work to solve specific problems in their countries, online territorial issues will be addressed in specific countries.

For instance, identity theft and scamming can be solved through strategies such as location tracking and VPN use (a form of forensic mobile and network solutions), which the same online fraudsters apply to reach their targets, (Koroniotis, Moustafa, & Sitnikova, 2019). Military and forensic interventions should provide policy interventions that help countries agree on what actions to take when the online privacy violation is inter-regional. Interventions, such as keeping security systems updated, using anti-viruses, and adjusting social media settings, do not offer long-term solutions. In addition, the solutions offer no reassurance that legal implications would follow. Future interventions must be integrated into all privacy violations.

Implications

Successfully implementing forensic solutions to the current problem will save individuals and businesses from financial and reputation damage. Adoption of fog nodes are crucial forensic solutions towards the reduction of online privacy issues. Fog computing offers several benefits that improve privacy, through its reduction of response time to decrement of data offloads in Cloud. Furthermore, low latency to geographical distributions are essential solutions that are primarily not supported by IoT applications. When people feel safe online, even internet service providers make profits. They must also be included in the research because privacy maintenance should be at the top of their priority list. If the military, forensic scientists and internet service providers work together, they will overcome the existing barriers and expand capacity for business growth at corporate and individual levels.

References

1. Abraham, W. K., Saravanan, S., & Smith, K. (2019, June). Security and Privacy Challenges in Fog Computing. In *International Conference on Fog Computing*.
2. Alzoubi, L. Y., Osmanaj, H. V., Jaradat, A., & Al-Ahmad, A. (2021). Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *Security and Privacy*; 4(2), e145, doi/10.1002/spy2.145
3. Atlam, H. F., Hemdan, E. E. D., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2020). Internet of things forensics: A review. *Internet of Things*, *11*, 100220.
4. Campbell, D. T., & Stanley, J. C. (2015). *Experimental and quasi-experimental designs for research*. Raven Books.
5. Choi, D. (2021). Digital Forensic: Challenges and Solution in the Protection of Corporate Crime. *The Journal of Industrial Distribution & Business;* 12(6), 47-55, doi/10.13106/jidb.2021.vol12.no6.47
6. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities.
7. Dhiman, A., Sen, A., & Bhardwaj, P. (2018). Effect of self-accountability on self-regulatory behaviour: A quasi-experiment. *Journal of Business Ethics*, *148*(1), 79-97.
8. Edmonds, W. A., & Kennedy, T. D. (2019). Quantitative Methods for Experimental and Quasi-Experimental Research. *An Applied Guide to Research Designs: Quantitative, Qualitative, and Mixed Methods. Thousand Oaks, CA: Sage*, 29-34.
9. Hasan, N., Chamoli, A., & Alam, M. (2020). Privacy challenges and their solutions in IoT. In *Internet of Things (IoT)* (pp. 219-231). Springer, Cham.
10. Joshi, R. C., & Gupta, B. B. (Eds.). (2019). *Security, Privacy, and Forensics Issues in Big Data*. IGI Global.
11. Keren, G. (2014). Between-or within-subjects design: A methodological dilemma. *A handbook for data analysis in the behavioral sciences*, *1*, 257-272.
12. Koroniotis, N., Moustafa, N., & Sitnikova, E. (2019). Forensics and deep learning mechanisms for botnets in internet of things: A survey of challenges and solutions. *IEEE Access*, *7*, 61764-61785.
13. Kumar, G., Saha, R., Lai, C. & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Generation Computer Systems*, 120, 13-25, doi/10.1016/j.future.2021.02.016

14. Lakshmi, S., & Mohideen, M. A. (2013). Issues in reliability and validity of research. *International journal of management research and reviews*, *3*(4), 2752.
15. Price, P. C., Jhangiani, R. S., & Chiang, I. C. A. (2015). Quasi-experimental research. *Research Methods in Psychology*.
16. Razi, A., Agha, Z., Chatlani, N., & Wisniewski, P. (2020, April). Privacy Challenges for Adolescents as a Vulnerable Population. In *Networked Privacy Workshop of the 2020 CHI Conference on Human Factors in Computing Systems*.
17. Reichardt, C. S., & In Little, T. D. (2019). *Quasi-experimentation: A guide to design and analysis*.
18. Singh, M., Halgamuge, M. N., Ekici, G., & Jayasekara, C. S. (2018). A review on security and privacy challenges of big data. In *Cognitive computing for big data systems over IoT* (pp. 175-200). Springer, Cham.
19. Stanley, T. D., & Jarrell, S. B. (2005). Meta-regression analysis: a quantitative method of literature surveys. *Journal of economic surveys*, *19*(3), 299-308.
20. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.
21. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.
22. Wang, L., & Fan, X. (1998). Six Criteria for Survey Sample Design Evaluation.
23. Wang, X., Ning, Z., Zhou, M., Hu, X., Wang, L., Zhang, Y., ... & Hu, B. (2018). Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions. *IEEE Communications Surveys & Tutorials*, *21*(2), 1314-1345.
24. Yuan, M., & Lin, Y. (2006). Model selection and estimation in regression with grouped variables. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, *68*(1), 49-67.
25. Qureshi, S., Li, J., Akhtar, F., Tunio, S., Khand, H. Z. & Wajahat A. (2021). Analysis of Challenges in Modern Network Forensic Framework. *Security and Communication Networks,* 1-13, doi/10.1155/2021/8871230.

تحديات الخصوصية على الإنترنت وحلول الطب الشرعي

بندر فقيها

قسم الخدمات الطبية الطارئة، كلية العلوم الصحية، جامعة أم القرى، المملكة العربية السعودية

bsfakiha@uqu.edu.sa

ملخص

في العالم الحديث، الذي يشار إليه بالعصر الرقمي، فإنّ عديداً من الأشخاص يدخلون إلى الأنترنت. ونادرًا ما يعرف متى يقوم شخص آخر بالتنصت، أو على وشك الاحتيال عليهم. فالشركات والمستخدمون الفرديون للمنصات عبر الإنترنت، جميعهم عرضة للانتهاكات الأمنية. وتتراوح تحديات الخصوصية عبر الإنترنت من الثقة والرقابة الهرمية إلى الخسائر المالية. ومع تقدم الأنظمة، يشعر الناس بالتفاؤل؛ فعلم الطب الشرعي سيوفر تدخلات طويلة الأجل، تتجاوز الحلول الحالية، والتي تشمل تعيين كلمات مرور قوية وجدار الحماية. ويتغير مستقبل الخصوصية عبر الإنترنت، ويجب مواءمة تدخلات أكثر واقعية لتجنب المشكلات التي تمت مناقشتها.

الكلمات الدالة: إنترنت الأشياء ، الخصوصية، الأمان، الأفراد، الشركات، التحديات، الحلول، المستخدمون.