Towards a Triad for Data Privacy

Quentin Covert
Dakota State University
Quentin.Covert@trojans.dsu.edu

Mary Francis
Dakota State University
Mary.Francis@dsu.edu

Dustin Steinhagen
Dakota State University
Dustin.Steinhagen@trojans.dsu.edu

Kevin Streff, Ph.D.
Dakota State University
Kevin.Streff@dsu.edu

Abstract

Data privacy is a topic of interest for researchers, data collection managers, and data system specialists. To assuage growing concerns regarding the collection and use of personal data, many organizations have begun developing systems and drafting policies meant to safeguard that data from potential privacy harms. This paper provides a surface-level comparison of data privacy triads from NIST in the United States and ULD in Germany that may form the basis for a future universal definition of data privacy. The analysis shows two different approaches for defining data privacy: one which focuses on the practical implementation of data privacy safeguards (NIST) and one that focuses on defining the highest possible standards to which data processors must be held (ULD).

1. Introduction

In January of this year, security experts discovered a massive security breach: a collection of 772 million unique emails and 21 million unique passwords [1]. These types of massive breaches are occurring more frequently, resulting in increased public and industry pressure to safeguard the privacy of users. While there are established standards related to security, privacy controls in the U.S. are still under development.

One thing holding back privacy is that a generally accepted and well-formed definition of data privacy (and, thus, that which must be protected) has not yet been developed. The purpose of this paper is to analyze two potential ontological definitions for data privacy while also providing recommendations to produce stronger definitions in the future. Without an agreed-to definition, how can data privacy standards, tools, and solutions be developed? Would a vendor-developed tool be missing an important component of data privacy? Would privacy assessors and auditors have incomplete standards from which to model after?

Information security is commonly understood to be made up of confidentiality, integrity and availability. This shared understanding of the definition of security allows vendors to build tools that can be consistently utilized by all organizations, regardless of culture, nationality, size and mission. Since data privacy currently lacks a standard definition, vendors run the risk of developing privacy standards, frameworks, checklists and tools which are fundamentally incomplete, ineffectual, or even harmful to the organizations that use them. This concern of continuing with a fractured understanding of data privacy begs the question of what actions standard-setting bodies have taken when it comes to formally defining the issue.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) is a data protection authority based in Kiel, Germany that advises data processors on data privacy-related issues. In 2015, the ULD published "Protection Goals for Privacy Engineering" as part of the IEEE CS Security and Privacy Workshops. In this report, the ULD defines six protection goals organized as a set of three axes. These three axes form their so-called Six-Pointed Star and form the basis of their ontology [43].

The National Institute of Standards and Technology is a United States Department of Commerce institute that supports American scientific innovation and industrial competitivity. In NIST Internal Report 8062, NIST introduced a data privacy framework to assist in the development of systems that better protect the privacy of those whose data is collected, stored, and retained in those systems. This document first appeared as a draft in January of 2015 before being published in April of 2017 with the intent to "establish the basis for a common vocabulary to facilitate better understanding and communication of privacy risk within federal systems, and the effective implementation of privacy principles" [2].

The remainder of this paper is as follows: section 2 contains a literature review regarding current data security and data privacy issues, section 3 details background information regarding the two frameworks being compared, section 4 contains the actual comparison and analysis of the ontologies, section 5 contains the conclusions reached as a result of the

URI: https://hdl.handle.net/10125/64277
978-0-9981331-3-3

comparison, and section 6 contains recommendations for future research regarding this topic.

2. Literature Review

Data breaches affected more than one billion people in 2018 [3]. In fact, reports demonstrate that data breaches of electronic health records are occurring on an unprecedented scale with half of the US population compromised [4]. Many annual data security studies exist examining the cybersecurity field [5-10]. Data breaches continue, and hackers consider data security big business.

Privacy breaches are also on the rise with data privacy becoming big business for hackers [11, 12]. Unfortunately, the Internet of Things (IoT) promises to magnify the number of privacy breaches [13]. With an ever-interconnected world, data privacy is an international issue [14-16]. Cambridge Analytica went into bankruptcy protection after their data handling practices came to light [17, 18]. Like the path of data security, the path of data privacy is being spearheaded by scandals, breaches, and international concern.

Consequently, data privacy is becoming a hot topic in business today [19-21]. At the U.S. federal level, NIST has created several "Security and Privacy" publications that address privacy assessments, privacy frameworks, and tips for privatizing technical environments [22-25]. Facebook has announced an enormous restructuring [26] and a change in strategy putting privacy at the center of their strategy [27]. But a simple question exists: what is data privacy? What constitutes data privacy? The world is creating privacy methods and tools to protect privacy [28], working to integrate privacy and technology [29], and has outlined key activities which must occur to keep a digital investigation private [30]. Diversity studies are completed to understand demographics behind good and poor privacy [31]. However, the reality is that the world pushed ahead with creating a plethora of privacy frameworks, tools, and solutions before it developed a universal understanding of what data privacy is [32, 33].

When it comes to privacy, however, most of the research done has been based on defining it in a legal or philosophic sense and, while these definitions are powerful, they do not define data privacy in the way the CIA triad defines data security [34]; [35]; [36]; [37]. A great deal of research and development has been conducted to define data security. From these efforts came a fairly universal understanding and the development of the CIA Triad [38]. The CIA triad highlights confidentiality, integrity and availability as the three primary goals of data security [39]. Because of this agreed-to definition, lawmakers, security professionals and policymakers all understand that data security is comprised of confidentiality, integrity and availability. Vendors can create solutions which address all three important goals.

While data security has much work to keep ahead of the bad guys, the definition is firm, and solutions can be developed and operationalized. When new technologies emerge (such as machine learning and artificial intelligence), these technologies can be targeted to all the characteristics of a triad (in the case of data security to the confidentiality, integrity and availability characteristics).

Data privacy does not have an agreed-to definition, so organizations run the risk of incomplete data privacy. Data privacy is considered a thornier issue than data security [40]; consequently, many policymakers simply avoid defining data privacy [33]. Many are putting their heads in the sand, but during a crisis, privacy and personal integrity issues can sometimes be overlooked [41]. Similar to data security, data privacy must be baked into organizational business processes [42]. As such, NIST has developed a series of publications to assist decision-makers and implementors with privacy processes and safeguards [22-25]. With no shared agreement of the key aspects that must be considered when developing systems and protocols to protect privacy, it is time to analyze those that are breaking ground in this area to move toward an understanding of a possible data privacy triad.

3. Background

A. The ULD Star

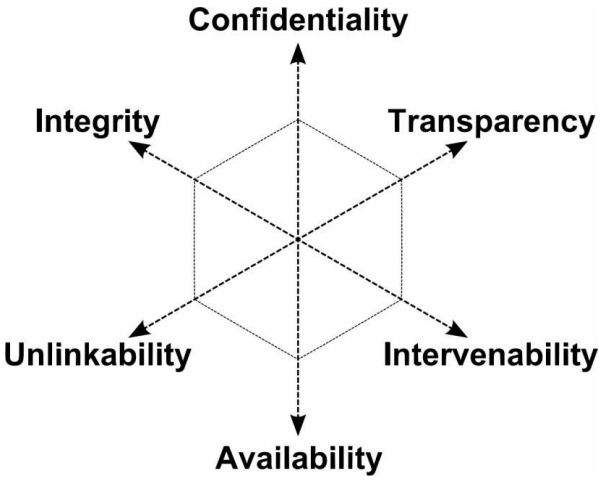

Figure 1 – The ULD six-pointed star

The ULD is a European government organization that specializes in privacy. Since the European Union is at the bleeding edge of privacy protections with their recent General Data Protection Regulation, it is reasonable to use a framework from a German data protection authority as a representative framework for many international communities. The three axes of the Six-Pointed Star include Confidentiality versus Availability, Integrity versus Intervenability, and Transparency versus Unlinkability [43].

Confidentiality, Integrity, and Availability are taken directly from the CIA security triad. The inclusion of the security triad objectives within the privacy structure highlights that, while security is an important component of privacy, it should be considered a subset of privacy. The additional aspects of privacy included by ULD are Intervenability, Transparency, and Unlinkability, which are defined by the ULD in the same publication.

Unlinkability is "the property that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context" [43]. If unlinkability is a priority, it should be nigh-impossible to link any information gathered to any information outside of the privacy system's domain. The ULD claims that "the most effective method for unlinkability is data avoidance" [43]. One should only collect, process, and store data when absolutely necessary.

Transparency is "the property that all privacy-relevant data processing… can be understood and reconstructed at any time" [43]. Anything a data processing system does regarding the collection, processing, storage, or future planned processing should be understood and reproducible by those using the system and those running the system.

Intervenability is "the property that intervention is possible concerning all ongoing or planned privacy-relevant data processing" [43]. Specifically, the report states, the data subjects themselves should be able to intervene with regards to the processing of their own data. This, according to the ULD, is a way of ensuring that data subjects have the ability to control how their data is processed and by whom.

B. The NIST Triad

The NIST privacy objectives, as defined in NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems, is an effort to provide "more guidance on privacy engineering processes, including the assessment of privacy risk" [2] and supplement the FIPPs (Fair Information Practice Principles) defined in US government's Circular A-130 document [44]. The document lists a set of three privacy objectives meant to be data privacy's version of the CIA triad. These objectives are predictability, manageability, and disassociability.

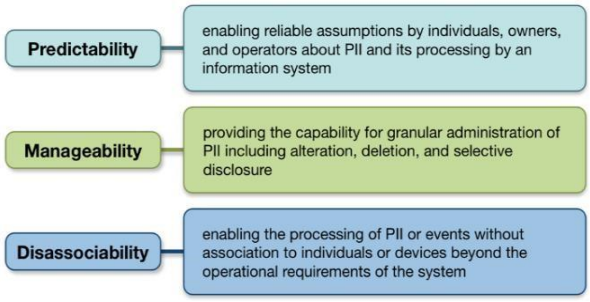

Figure 2 – The NISTIR 8062 privacy objectives

Predictability is defined as "enabling reliable assumptions by individuals, owners, and operators about PII (Personally Identifiable Information) and its processing by an information system" [2]. This objective, according to NIST, helps to ensure the FIPPs of Accountability, Authority, Purpose Specification and Use Limitation, and Transparency. To summarize the definition, predictability is the notion that those interacting with the system (whether they be operating or using it) has the ability to make reasonable assumptions about how the system handles PII. While this objective does encourage transparency, it does not require complete transparency. It simply aims to ensure that anyone using the system is not surprised by how it handles data.

Manageability is defined as "providing the capability for granular administration of PII including alteration, deletion, and selective disclosure" [2]. The FIPPs of Accountability, Minimization, Quality and Integrity, and Individual Participation are supported by Manageability, according to NIST. By way of manageability, those who process PII are able to ensure the accuracy of data and the prompt removal of obsolete information, while also ensuring that only necessary information is collected and disclosed. Manageability does not, however, state that all individuals should have "the right to control their information, although it could enable a system capability to implement that policy" [2]. This distinction is made because some systems handle information about data subjects that the subjects should not be allowed to change, such as tax information handled by the IRS.

Disassociability is defined as "enabling the processing of PII or events without association to individuals or devices beyond the operation requirements of the system" [2]. This objective helps to

supplement two FIPPs: Accountability and Minimization, according to NIST. In essence, this objective aims to ensure that systems protect data subjects from the unnecessary exposure of PII: data should be disassociated from the subjects the data comes from whenever possible. NIST does not, however, claim that disassociability and anonymity are equivalent. Namely, NIST states that "agencies may opt to knowingly accept the risk [of exposure], or select controls that require an acceptance of greater residual risk…" Unlike confidentiality, which is focused on preventing unauthorized access to information, disassociability recognizes that privacy risks can result from exposures even within an authorized perimeter.

4. Analysis

A cursory inspection of the two frameworks shows a clear connection: namely, predictability is mappable to transparency, unlinkability is mappable to dissasociability, and manageability is mappable to intervenability. Predictability and transparency both stipulate that the system be understandable and predictable from an outsider's perspective.

Unlinkability and dissasociability both require that any information used and stored be unconnectable to outside information, and both frameworks state that the best method to ensure their respective principle is to minimize the data collected. Manageability and intervenability both state that data should be correctable by the proper parties. However, a more thorough examination reveals critical differences between the two.

A. Predictability versus Transparency

Figure 3 – Visual representation of transparent systems as a subset of predictable systems

With regards to predictability and transparency, the degree to which a system should be understood from an outside perspective is drastically different. Predictability is met if "reliable assumptions" can be made about the system in question [2]. This does not implicitly mean that data subjects and stakeholders know how the data is being used, but rather that subjects and stakeholders are not *surprised* by the way data is used. Transparency, on the other hand, requires that any data processing system should be understandable and *reconstructable* at any given time [43].

To put it another way, predictable systems are black boxes: if one puts information in, the outcome of that data entry is predictable by data subjects and shareholders alike. Transparent systems are essentially white boxes: while the ULD make no specific mention to a complete understanding of the system's technical details, the fact that all transparent systems must be reproducible implies a degree of system visibility far exceeding the requirements of predictable systems. Following this comparison, one could state that transparent systems are a subset of predictable systems.

Additionally, transparency requires that a multitude of contexts regarding the system in question be understandable and reconstructable, "including the legal, technical, and organization setting" [43]. Predictability makes no such mention of the context in which the system is used. Once again, this lends credence to the idea that predictable systems are a subset of transparent systems. While the technical capabilities of the system must be made apparent to users in a predictable system, the context in which the system is used need not be made apparent.

As an example, say a company collected, stored, and processed PII. This company states that the system they use gathers user-submitted data, stores it in on-site servers, and then uses that information to better tailor the services they provide to the individual user. What they do not mention is that they tailor their services by sharing this information to a politically affiliated association which then uses that information to target users with political advertisements. This system would be a predictable one, but not a transparent one.

It is technically true that the information is used to tailor the services the company provides to the individual user, and it does so is an unsurprising way. However, a transparent system would be required to state how the information is used specifically as part of its privacy notice: In this case, not disclosing that personal data would be used for targeted advertising is a privacy-relevant detail in the organizational setting context. Since it wasn't disclosed beforehand (and hence the data processing wasn't understood "at any time" as per ULD), it is a violation of the transparency protection goal.

When it comes to implementing one of these two objectives into a data processing system, both have their pros and cons. As may be obvious, transparency is

stricter than predictability, and it is therefore more costly to implement in terms of energy, time, and money. However, one could see the choice as the difference between a system that your customers can trust and a system that your customers can understand. In many ways, this makes transparency the superior choice to predictability, as it can help sow good will that may or may not be available in a predictable system.

The managerial implications of these two objectives also highlight a key difference between the philosophies that motivated the development of these two partial ontologies. NISTIR 8062 is a government document meant to provide "future guidance on how federal agencies will be able to incorporate privacy as an attribute of trustworthy systems through the management of privacy as a collaborative, interdisciplinary engineering practice" [2]. By comparison, "Protection Goals for Privacy Engineering" states "The intention of this paper is to give an overview and some pointers to ongoing research in this area" [43]. It is, then, only natural for the NIST objective to choose a more cost-effective solution, while the ULD pushed the idea of predictability and similar concepts to their logical conclusions.

B. Manageability versus Intervenability

Figure 4 – Visual representation of intervenable systems as a subset of manageable systems

With regards to manageability and intervenability, once again it appears that the ULD framework is more restrictive than the NIST framework. Intervenability requires that data subjects be able to intervene during data processing and ensure that they are able to correct and erase data, withdraw consent to data collection and processing, and lodge claims and raise disputes to remedy wrongful uses of data [43]. By contrast, NIST explicitly states that "manageability is not a policy statement about whether individuals should have the right to control their information" [2].

To better visualize this comparison, consider a data broker. A data broker embracing intervenability would allow for complete modification and deletion of the data belonging to a data subject. If this data broker, alternatively, embraced manageability, the system could then be developed such that only internal staff could granularly perform administrative actions on the data.

If the system implements a way to modify data (given proper authorization), then the system would still "[provide] the capability for granular administration of PII including alteration, deletion, and selective disclosure" [2] thereby meeting the goal of manageability. Full intervenability requires that any subject whose data is stored in the system be able to modify that data, while manageability only requires that some qualified authority be able to do so.

When choosing between manageability and intervenability, one should first consider the nature of the data being processed and the way in which that data is used. If the data are going to change rapidly then consider intervenability. Should the data instead be relatively stable or if the data are highly sensitive and changes to the datum could result in drastic changes to how that datum is handled, consider manageability. Ultimately, one should consider how the data are likely to change over the course of its use and who should be able to correct and remove said data.

C. Disassociability versus Unlinkability

Figure 5 – Visual representation of disassociability and unlinkability

The differences between dissasociability and unlinkability are more subtle than in the other two comparisons. That is to say, there are very few actual differences between the two privacy goals. The two goals attempt to, in the words of NIST, "actively [protect] or ["blind"] an individual's identity or associated activities from exposure" [2] and require that system developers carefully consider the potential damages that could occur as a result of data exposure.

The confusing aspect of this, however, is the way in which the ULD defines unlinkability. In accordance with its name, unlinkability "is defined as the property that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context" [43]. This definition requires a careful consideration of what data is used and how that data is stored with the end goal of a data set that is unlinkable to domains and contexts outside of the current domain.

The keyword, for this comparison, is domain. One could make the argument that the use of this word implies that the data used should be linkable to similar domains outside of the data system itself. However, this contradicts the ULD's statement saying that their definition of unlinkability encompasses the concepts of data minimization and anonymity. Assuming that any interpretation of a definition that contradicts that definition is invalid, this means that unlinkability would not allow this linkability.

Thus, the major difference between the two definitions, the use of the term domain, is negligible. This implies that the two have goals so similar that they are practically indistinguishable from each other. Further analysis of these two privacy goals may reveal some subtle differences beyond the scope of this discussion, but for the purposes of this discussion, the two are the same concept said with slightly different words.

D. Holistic Comparisons

When taken as a whole, both frameworks call for some degree of security, anonymity, transparency, and data controllability. Both frameworks bring attention to the importance of the CIA triad, with NIST stating that the triad is the set of objectives by which systems meet the FIPP of Security and the ULD incorporating confidentiality, integrity, and availability into the Six-Pointed Star. Although they differ in subtle ways, each of the objectives have similar goals when compared to their counterpart in the other framework, as elaborated on at the start of section III.

The two frameworks also differ in structure. While the NIST framework's objectives are intended to be the CIA triad of privacy, the ULD triad is more than a triad. The Six-Pointed Star that transparency, unlinkability, and intervenability come from is a set of axes showing what a system prioritizes.

Given the relationships between the two goals, it is safe to say that the ULD triad focuses on defining the highest possible standards to which data processors must be held, while NIST's triad focuses more on the practical implementation of data privacy safeguards.

Put another way, one could say that the three objectives of the NIST triad are goals that are capable of defining how well a system supports the privacy policies of an organization while the Six-Pointed Star assumes that some kind of balance between security, privacy, and goals within security and privacy will always be reached by data systems and provides a way of visualizing and measuring the tradeoffs made during the system's development.

5. Conclusions

Privacy is a complex topic that is enjoying more and more research and development in recent years. As part of this research, frameworks that are useful in analyzing information system privacy goals and objectives are a natural development. By comparing these frameworks, subtle differences related to the extent to which each part of the framework accurately measures privacy and the components of privacy each framework part attempts to address emerge. In this comparison, it is clear that the intent behind the framework influences its design.

As the preceding analysis shows, the Six-Pointed Star developed by the ULD has much stricter requirements regarding what must be done to safeguard the privacy of data subjects. Both transparency and intervenability define systems that form a proper subset of systems within systems defined by their NIST counterparts: predictability and manageability. By comparison, NIST-defined systems are generally easier to implement: the cost of turning a predictable system into a transparent one tends to be non-trivial, for example.

Given the two different goals found in the holistic comparisons between the two, it is difficult to say which is objectively superior as each framework has a set of goals that are not directly compatible with each other. While many ideas are represented in both frameworks, the differences in practicality, usability, strictness, and intent make the two too distinct to directly compare their quality. Neither framework, then, is inherently superior to the other in all scenarios.

However, the framework proposed by the ULD would make a stronger starting point for the definition of data privacy because of its focus on defining the highest possible standards that data processing organizations must follow. A universal definition for data privacy must be as all-encompassing as is possible, and the practical implementation focus of NIST's framework, while important for the implementation of data privacy, was found to be less restrictive comparatively. However, the ULD standard is incomplete because it does not take into account compromises which are necessary if the definition is to be used in the future. That is to say, while the ULD standard is a better basis for a future definition, it must

be expanded to include the considerations included in the NIST framework.

6. Recommendations and Future Work

Given that the Six-Pointed Star is the stronger starting point for a universal definition of data privacy, future work expanding on this comparison should center around enhancing the ULD framework to mitigate its weaknesses with regards to the implementation of its objectives.

The two triads used in this analysis are not universally accepted as definitive and comprehensive definitions of data privacy, as evidenced by the numerous other frameworks that have been developed. In future research, comparisons between the frameworks used in this analysis and other data privacy frameworks and any potential triads such as the EU's GDPR, APEC's Privacy Framework, and Google's Framework for Responsible Data Protection [45]; [46]; [47] should be performed. Additionally, this research will help to pave the way for a universal definition of data privacy and an accepted set of principle components of data privacy.

Given the fact that these frameworks were defined by different countries, future research should also be performed to determine the differing notions, goals, and intentions that lead to the development of data privacy frameworks in different countries and cultures. Building on this idea, any research into currently enacted privacy laws or regulations would be invaluable towards reaching a common data privacy triad.

Finally, as this comparison is relatively shallow with regards to the full reports that define these privacy triads, a deeper dive into the way in which these privacy triads are to be implemented or an exhaustive comparison and analysis between the two frameworks as a whole would be useful for future discussions.

7. References

[1] A. Jain, "ValueWalk: Massive Data Breach Exposes 773M Emails; Check If You Are Safe Or Not," in *Newstex Global Business Blogs*, N. G. B. Blogs, Ed., ed. Chatham: Newstex, 2019.

[2] S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau, "An introduction to privacy engineering and risk management in federal systems," National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8062, 2017/01// 2017, [Online]. Available:https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf, Accessed on: 2019/04/08/02:29:19.

[3] A. Barratt. (2019). *2019 is the year we discover the true cost of poor data protection* [Online]. Available: https://www.techradar.com/news/2019-is-the-year-wediscover-the-true-cost-of-poor-data-protection.

[4] W. W. Koczkodaj, M. Mazurek, D. Strzałka, A. WolnyDominiak, and M. Woodbury-Smith, "Electronic Health Record Breaches as Social Indicators," (in English), *Social Indicators Research*, vol. 141, no. 2, pp. 861-871, Jan 2019.

[5] "One-Third of Ransomware Victims Pay Associated Ransoms, Finds '2017 Cyberthreat Defense Report'," in *Business Wire*, ed. New York, 2017.

[6] "How to build a more effective cybersecurity culture," (in English), *SecurityInfoWatch.com*, 2017 Feb 24.

[7] "Cisco Brings Out 2017 Annual Cybersecurity Report," (in English), *Manufacturing Close - Up*, 2017 Feb 08.

[8] "Cybersecurity Industry," Acquisdata Pty Ltd, Yass, 2018 Dec 03 2018, [Online]. Available: https://search.proquest.com/docview/2162339489?accountid =27073.

[9] Y. Martin and A. Kung, "Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering," in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 2018, pp. 108111.

[10] "IBM publishes "The 2019 Cyber Resilient Organization"- the fourth annual benchmark study on Cyber Resilience-an organisation's ability to maintain its core purpose and integrity in the face of cyberattacks," in *Insurance Newslink*, ed. Farnham, 2019.

[11] S. Butler, "Privacy is Big Business," O. M. a. F. I. Forum, Ed., ed, 2018.

[12] A. Vetter. (2019). *Invading Your Privacy Is Big Business: Facebook Now Worth More Than Wal-Mart* [Online]. Available: https://americans.org/invading-yourprivacy-is-big-business-facebook-now-worth-more-than-walmart.

[13] H. Peter Buell, "The goose that laid the golden eggs: personal data and the Internet of Things," (in English), *The Journal of Business Strategy*, vol. 40, no. 1, pp. 48-52, 2019.

[14] S. Agarwal and D. Sengupta, "FB breach: Privacy advocates in India seek stronger data laws [Internet]," in *The Economic Times*, ed. New Delhi, 2018.

[15] C. Stupp, "European Privacy Regulators Find Their Workload Expands Along With Authority; Facing prospect of steep fines, companies report minor breaches beyond scope of GDPR," (in English), *WSJ Pro. Cyber Security*, 2019 Apr 12.

[16] J. Williams, "Panelists Offer Views on Data Privacy Legislation," (in English), *Cybersecurity Policy Report*, p. 1, 2019 Feb 11.

[17] K. Martin, "Cambridge Analytica Files for Chapter 7 Bankruptcy," in *FoxBusiness*, ed, 2018.

[18] N. Confessore and M. Rosenberg, "Cambridge Analytica to File for Bankruptcy After Misuse of Facebook Data," in *The New York Times*, ed, 2018.

[19] R. McQueeney, "Zacks Investment Research: Why User Privacy Will Be the Hottest Tech Topic of 2018," ed. Chatham: Newstex, 2017.

[20] L. Kalman, "New European Data Privacy and Cyber Security Laws– One Year Later," (in English), *Association for Computing Machinery. Communications of the ACM*, vol. 62, no. 4, p. 38, Apr 2019.

[21] M. Miller, "FTC's role in regulating data privacy is hot topic at SXSW tech conference," (in English), *Inside Cybersecurity*, 2019 Mar 12.

[22] NIST, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans" in "SP 800-53 R4," 2015.

[23] NIST, "Security and Privacy Controls for Information Systems and Organizations" in "SP 800-53 R5," 2017.

[24] NIST, "NIST Big Data Interoperability Framework: Volume 4, Security and Privacy Version 2," 2018.

[25] NIST, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy", 2018.

[26] E. Dreyfuss, "Facebook Hires Up Three of its Biggest Privacy Critics," Wired.com, Ed., ed, 2019.

[27] (2019). *Is the new 'privacy-focused' strategy the reason behind Facebook exodus*.

[28] Y.-S. Martin and A. Kung, "Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering," presented at the 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) 2018.

[29] A. Sokolovska and L. Kocarev, "Integrating Technical and Legal Concepts of Privacy" *IEEE Journals & Magazines* vol. 6, pp. 26543 - 26557, 2018.

[30] A. Dehghantanha and K. Franke, "Privacy-respecting digital investigation " presented at the 2014 Twelfth Annual International Conference on Privacy, Security and Trust 2014.

[31] Q. Wang and X. Shi, "(a, d)-Diversity: Privacy Protection Based on l-Diversity," presented at the 2009 WRI World Congress on Software Engineering 2009.

[32] T. Weimann and D. Nagel, "Agreeing on a Definition for Data Protection in a Globalized World" *IEEE Technology and Society Magazine* vol. 31, no. 4, pp. 39-42, 2012.

[33] C. J. Castelli, "NIST's draft privacy-engineering concepts avoid defining privacy," (in English), *Inside Cybersecurity*, 2014 Oct 07.

[34] R. Calo, "Privacy and Markets: A Love Story," *Notre Dame Law Review*, vol. 91, no. 2, 2016.

[35] D. J. Solove, "A Taxonomy of Privacy," (in en), *University of Pennsylvania Law Review*, vol. 154, no. 3, p. 477, 2006/01/01/ 2006.

[36] H. Nissenbaum, "Contextual Approach to Privacy Online," *Dædalus*, vol. 140, no. 4, pp. 32-48, 2011.

[37] A. Westin, "Social and Political Dimensions of Privacy," *Journal of social issues*, vol. 59, no. 2, pp. 431453, 2003.

[38] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," presented at the 2013 International Conference on Availability, Reliability and Security, 2013.

[39] K. Fenrich. (2008). *Securing your control system: the 'CIA triad' is a widely used benchmark for evaluating information system security effectiveness*.

[40] T. Leithauser, "ON PRIVACY, NIST OFFICIALS CONFRONT THORNIER ISSUE THAN CYBERSECURITY," (in English), *Cybersecurity Policy Report*, p. 1, 2014 Apr 14.

[41] J. S. Hiller and R. S. Russell, "Privacy in Crises: The NIST Privacy Framework," (in English), *Journal of Contingencies and Crisis Management*, vol. 25, no. 1, pp. 3138, Mar 2017.

[42] N. Lomas, "Coding In The Cloud Era Demands A Structural Rethink To Bake In Security And Privacy," (in English), *TechCrunch*, 2015 Sep 27.

[43] M. Hansen, M. Jensen, and M. Rost, "Protection Goals for Privacy Engineering," in *2015 IEEE Security and Privacy Workshops (SPW)*, 2015, San Jose, CA: IEEE, pp. 159-166. [44] Office of the Federal Chief Information Officer, "CIRCULAR No. A-130," 2016.

[44] "General Data Protection Regulation (GDPR) Regulation (EU) 2016/678," ed. European Union, 2016.

[45] Asia-Pacific Privacy Corporation, "APEC Privacy Framework," 2005.

[46] Google, "Framework for Responsible Data Protection Regulation," 2018.