

2-7-2024

Privacy Principles and Harms: Balancing Protection and Innovation

Samuel Aiello

Dakota State University, sam.aiello@trojans.dsu.edu

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/jcerp>



Part of the [Information Security Commons](#), [Management Information Systems Commons](#), and the [Technology and Innovation Commons](#)

Recommended Citation

Aiello, Samuel (2024) "Privacy Principles and Harms: Balancing Protection and Innovation," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 15.

DOI: <https://doi.org/10.62915/2472-2707.1167>

Available at: <https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/15>

This Article is brought to you for free and open access by the Active Journals at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Privacy Principles and Harms: Balancing Protection and Innovation

Abstract

In today's digitally connected world, privacy has transformed from a fundamental human right into a multifaceted challenge. As technology enables the seamless exchange of information, the need to protect personal data has grown exponentially. Privacy has emerged as a critical concern in the digital age, as technological advancements continue to reshape how personal information is collected, stored, and utilized. This paper delves into the fundamental principles of privacy and explores the potential harm that can arise from the mishandling of personal data. It emphasizes the delicate balance between safeguarding individuals' privacy rights and fostering innovation in a data-driven society. By analyzing key privacy principles and their implications, this paper explores the foundational privacy principles that define the concept of privacy while delving into the potential harms that can arise when these principles are violated.

Keywords

Privacy protection, personal data, privacy violations, privacy rights, privacy harms, privacy principles, privacy laws

Privacy Principles and Harms: Balancing Protection and Innovation

Sam Aiello

Beacom College of Computer and Cyber Sciences

Dakota State University,

Madison, South Dakota USA

sam.aiello@trojans.dsu.edu

ORCID- 0000-0002-1260-7227

November 25, 2023

ABSTRACT

In today's digitally connected world, privacy has transformed from a fundamental human right into a multifaceted challenge. As technology enables the seamless exchange of information, the need to protect personal data has grown exponentially. Privacy has emerged as a critical concern in the digital age, as technological advancements continue to reshape how personal information is collected, stored, and utilized. This paper delves into the fundamental principles of privacy and explores the potential harm that can arise from the mishandling of personal data. It emphasizes the delicate balance between safeguarding individuals' privacy rights and fostering innovation in a data-driven society. By analyzing key privacy principles and their implications, this paper explores the foundational privacy principles that define the concept of privacy while delving into the potential harms that can arise when these principles are violated.

Index Terms— Privacy protection, personal data, privacy violations, privacy rights, privacy harms, privacy principles, privacy laws

I. INTRODUCTION

With data security threats on the rise, individuals rightfully demand privacy rights be upheld alongside digital advancement. However, achieving this balance involves overcoming discrepancies between privacy expectations and

actual security practices. As innovations generate new data flows, they often enable unintended privacy consequences. Without commensurate protections in place proactively, vulnerabilities emerge that leave consumers distressed and organizations noncompliant.

The theme of this paper is to explore the crucial role of privacy principles, laws, and protections in the contemporary digital landscape. As connectivity proliferates along with data collection, safeguarding personal information is paramount yet increasingly complex. Core research questions arise- *How do we balance innovation and privacy? What constitutes responsible data handling? How do we mitigate privacy harms?* By examining key privacy frameworks, risks, and regulations, this manuscript seeks to interpret ethical imperatives and legal responsibilities around personal data in our technology-driven age and aims to further awareness and dialogue around constructing ethical yet innovative data systems.

Responsible progress demands examining where strategies succeed versus engender mistrust. With diligence and collaboration, privacy rights and technological promise need not be mutually exclusive. Our interconnected future relies on this commitment.

II. DISCUSSION

Numerous nations have implemented privacy legislation, such as the General Data Protection

Regulation (GDPR) (1) in Europe and the California Consumer Privacy Act (CCPA) (2), which mandate that corporations secure legitimate consent and grant individuals' authority over their personal information. The promotion of transparency and competent data processing fosters confidence among individuals and organizations by facilitating consent and control. By granting individuals autonomy over their data, corporations are motivated to adopt comprehensive data security protocols to safeguard said data.

A. Privacy Principles

In the ever-evolving landscape of digital connectivity, where information flows seamlessly across vast networks, the principle of data minimization stands as a vital beacon of responsible data handling. At its core, data minimization champions the idea that less is often more—only the bare minimum of personal data necessary should be collected and processed for a specific purpose. This foundational principle serves as a linchpin in the realm of data protection, underpinning the ethical and legal safeguards that are increasingly crucial in our contemporary digital era. As we explore the essence of data minimization and its pivotal role in preserving privacy rights, we also delve into the broader framework of consent and control—two fundamental principles that empower individuals to navigate the digital landscape with autonomy and informed choices. In this exploration, we shed light on the ethical imperative of upholding individual autonomy and choice while championing data minimization as a cornerstone in the protection of personal information.

The principle of data minimization dictates that only the minimum amount of personal data necessary for a specific purpose should be collected and processed. This principle is essential in reducing the risk of excessive data exposure and ensuring that individuals retain control over their information.

In Article 5 of the GDPR, there is a list of the most important data security rules that must be followed when handling personal information. It

includes minimizing data, which is also called "data avoidance". The GDPR specifies that personal information must be "adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed." This means that you must follow some prescriptive guidelines. The way the data is collected must make sense for the goals of processing. But it is not enough that collecting a certain type of data is necessary to reach the goal of processing. The principle of data minimization also says that this collection must be required.

The safeguarding of individuals' privacy rights and prevention of unauthorized disclosure (3) or exploitation of personal information heavily rely on the principles of consent and control. In the contemporary era of digital technology, it is vital from an ethical standpoint to uphold and preserve an individual's autonomy and choices. The protection of someone's privacy is based on two fundamental principles: consent and control. They give individuals the ability to make educated decisions about the use of their personal data and ensure that companies handle data in an ethical and responsible manner. Understanding and adhering to these principles is essential for a society that places a high value on protecting individuals' privacy as the digital landscape continues to undergo rapid transformation.

i. Consent for Privacy

When discussing privacy, the term "consent" refers to an individual's decision to provide permission knowingly and willingly to an organization or entity to collect, handle, and distribute their personal information. This agreement must be made in an informed manner. Obtaining informed consent (4) from individuals before collecting their data is a cornerstone of privacy protection. It empowers individuals to exercise control over their personal information and enables them to make informed decisions about its usage.

The main points are as follows:

- Voluntary- Consent must be given voluntarily, without coercion or pressure.

- Informed- Individuals must be given plain and comprehensible information about the data being collected, how it will be used, and who will have access to it.

- Specific- Consent should be specific to the intended use of the collected data. Blanket, or generic consent is not considered legitimate.

- Revocable- Individuals should have the right to revoke their assent at any time without incurring any negative consequences.

Consent in various contexts can vary by authority and context, especially in healthcare, financial and credit card processing, online services, and advertising.

In the context of privacy, the term "control" refers to an individual's capacity to govern and direct the way their personal information is gathered, utilized, and kept, as well as how it is shared with third parties.

The essentials are as follows:

- Data Minimization: Control incorporates the principle of data minimization, which states that organizations should only collect the minimum amount of data required to achieve their stated goals.

- Access and Correction: Individuals should have the right to access and rectify their personal information held by organizations.

- Data Portability: Control also includes the capacity to transfer personal information from one service or organization to another.

- Individuals typically have the right to request the deletion of their data when it is no longer required or when consent is withdrawn.

- Notification: Organizations are required to promptly notify individuals about data breaches or unauthorized access.

At the time of collection, an individual should be informed of the acceptable purposes for which

their personal data will be collected and utilized before the data is acquired. (5) Violating the privacy expectations of individuals is a risk that arises when these aims are not followed. Concurrently, it is the responsibility of companies to put in place adequate security measures to protect acquired data from being accessed by unauthorized parties, being compromised, or being leaked. The failure to protect sensitive data can result in serious violations of privacy.

B. Is Privacy an Ethical Issue or a Fundamental Human Rights Issue?

Privacy is both an ethical issue and a fundamental human rights issue. However, these two concepts are distinct in important ways:

Ethical rights refer to moral rights and entitlements that individuals should have in accordance with ethical principles and values. These ethical rights can include privacy, but they are based on normative judgments about what is morally correct rather than on legal recognition. There can be debate around ethical rights.

In contrast, fundamental human rights are established in international laws and treaties as basic rights that all humans should enjoy simply by virtue of being human. They are considered universal, inalienable, and legally enforceable entitlements under global human rights frameworks. The right to privacy is recognized as a fundamental human right in the UN Declaration of Human Rights and in other major human rights conventions.

So, while privacy is an ethical right in the sense that ethical reasoning and theories argue for individuals' entitlement to privacy as a matter of ethical justice, it is also a legally enshrined fundamental human right within international human rights law. All humans have a basic, inalienable right to privacy under this body of law.

The key difference is that fundamental human rights create binding legal obligations on states to respect and protect individuals' privacy through legislation and enforcement mechanisms. In contrast, ethical rights to privacy cannot be directly

enforced against states in this manner, even if we can make strong ethical cases that respecting privacy is the morally proper thing to do.

In summary, privacy is both an issue of ethical rights in terms of moral reasoning, and a fundamental human rights issue in terms of binding laws and international legal frameworks. It is a combination of ethical force as well as legal force.

C. Privacy Harms

Striking a balance between privacy protection and technological innovation is a complex task. While stringent privacy measures can impede data-driven innovation, the absence of privacy safeguards (6) can lead to significant harm. Organizations and policymakers must collaborate to develop privacy-enhancing technologies and frameworks that enable innovation while respecting privacy rights. Privacy is widely recognized as a basic human right in the United Nations Declaration of Human Rights, (7) as well as in many national constitutions and legal frameworks.

Privacy rights serve important individual and societal purposes- they allow people safety, dignity, and space for self-development away from judgment or interference. Infringements on privacy can leave individuals feeling violated and undermine personal autonomy. However, it must also be recognized that there has been immense value that technological innovation has brought to society in areas like healthcare, education, financial inclusion and beyond. New technologies often require some degree of data sharing to function, which interacts directly with privacy.

There are reasonable arguments on both sides- for more privacy safeguards to protect individuals, and for enabling responsible data use to allow continued innovation. Each new technology brings its own privacy implications that must be weighed carefully. Regulators strive to employ proportionate privacy protections tailored to specific technologies and use cases. But there remains reasonable disagreement on where lines should be drawn.

An open, ethical and public debate around concepts like data minimization, de-identification, transparency and consent are needed to navigate this debate. Tradeoffs may be unavoidable, but policy innovations like privacy-enhancing technologies (8) and ethical data impact assessments (9) can help mitigate the downsides. Above all, human well-being should remain the guiding principle. Privacy and innovation involve inherent trade-offs rather than clear binary choices. Ethics and proportionality are critical- while privacy rights can facilitate innovation by building public trust, unchecked data collection can violate autonomy.

A person's reputation (10) can be damaged by the dissemination of inaccurate personal information, hence protecting one's privacy is equally related to protecting one's reputation. Inaccurately and hurtfully portraying another person is a violation of their right to privacy, which is recognized under the common law torts. It is necessary for there to be a publication that was created with true malice, casts the victim in an unfavorable light, and would be extremely offensive to a reasonable person. False light privacy, on the other hand, is more concerned with safeguarding the mental and emotional health of the victim, in contrast to traditional defamation, which centers on causing harm to a person's reputation. When it comes to defamation, the truth can be used as a defense; nevertheless, if someone uses genuine facts to create a false implication, they are still committing the act of lying.

Nissenbaum (11), who coined the term contextual integrity, points out that it is possible for information to cause harm if it is obtained by the wrong people or if access to it is not controlled. The damage in question can be severe, as demonstrated by the fact that the assailant in the case of the murder of actor Rebecca Schaeffer in 1989 was able to locate her home location by consulting records kept by the Department of Motor Vehicles. Less tangible but no less important are harms such as identity theft, which is occurring with an increasing regularity, reportedly because of the ready availability of vital identifying information

such as Social Security numbers, addresses, and phone numbers. This type of crime is committed by those who gain access to a victim's personal information and use it to steal their identity. Furthermore, numerous products such as job, life, and medical insurance may be placed in jeopardy if the flow of medical information were not limited, or if information regarding people's religious and political affiliations, sexual orientation, or criminal records were widely available. This is because such information could be used to discriminate against individuals.

i. Typologies of Privacy Harms

Citron and Solove (12) focus on the many ways that people might be harmed by violations of privacy, and these categories attempt to capture them all. Privacy violations can result in various types of harms, including:

- physical,
- economic,
- reputational,
- psychological,
- autonomy,
- discrimination, and
- relationship

Physical harms involve physical harm to an individual's well-being, such as stalking or harassment. Economic harms involve financial losses or adverse consequences, such as identity theft or financial fraud. Reputational harms involve false accusations or defamation of an individual's personal information. Psychological harms involve emotional and mental distress due to privacy violations, such as anxiety, stress, humiliation, or loss of control. Autonomy harms limit an individual's ability to make informed decisions without external interference. Discrimination harms occur when personal information is used to categorize or profile individuals based on protected characteristics. Relationship harms involve

negative impacts on personal or professional relationships due to privacy breaches, such as trust erosion, damaged interpersonal connections, or severed professional ties.

D. Privacy Laws

Global privacy laws govern the collection, use, and protection of personal data, ensuring that individuals' privacy rights are respected and their data is handled responsibly. In an interconnected world, understanding these laws is essential for individuals, organizations, and governments. The table below provides an overview of global privacy laws, their key principles, and their impact.

Individuals are better protected from unwanted data access, breaches of their personal information, and the exploitation of their data thanks to global privacy regulations, which play an essential part in this protection. Compliance with these regulations is not just a best practice but a legal duty, and companies who fail to satisfy their duties face serious consequences. Compliance with these rules is not just best practice but a legal requirement. Penalties may consist of monetary fines, harm to one's reputation, and a breakdown in the relationship between the business and its customers. As the number of people concerned about their privacy continues to rise, it is critical for individuals as well as organizations to maintain a level of awareness regarding the ever-changing environment of worldwide privacy legislation. In today's hyper-connected world, individuals can take preventative measures to guarantee the safety of their personal data by routinely examining the privacy settings of online platforms and being informed about the evolution of laws governing privacy by monitoring changes to these laws. **Table 1** below summarizes some of the global privacy laws.

Key Global Privacy Laws (1, 2, 13, 14, 15)

| General Data Protection Regulation (GDPR) | |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authority | European Union (EU) and European Economic Area (EEA) |
| Features | GDPR is one of the most comprehensive privacy regulations globally, setting high standards for data protection, including strict consent requirements and substantial fines for non-compliance. |
| California Consumer Privacy Act (CCPA) | |
| Authority | California, United States |
| Features | CCPA grants California residents' rights over their personal information, including the right to know what data is collected and the right to opt-out of data sales. |
| Personal Information Protection and Electronic Documents Act (PIPEDA) | |
| Authority | Canada |
| Features | PIPEDA governs the collection, use, and disclosure of personal information by private-sector organizations, emphasizing consent and accountability. |
| Personal Data Protection Act (PDPA) | |
| Authority | Singapore |
| Features | The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure, and care of personal data. |
| Personal Information Protection Act (PIPA) | |
| Authority | South Korea |
| Features | PIPA applies to the protection of personal information and to provide a right of access to an individual's personal information. |

Table 1

Challenges arise when it comes to impact and compliance. Privacy regulations, such as the General Data Protection Regulation (GDPR), have a global reach, which means they can affect organizations worldwide if they process the data of EU citizens. This has led to a global movement towards enhancing privacy protections. However, organizations often face substantial compliance costs. These expenses may include hiring Data Protection Officers (DPOs), conducting privacy impact assessments, and drafting data protection policies. Additionally, some countries require data to be stored within their borders, which can pose a

challenge for businesses with a global presence. Moreover, many privacy laws mandate the immediate notification of relevant authorities and affected individuals in the event of a data breach; this is known as a data breach notification. Understanding these types of privacy harms helps highlight the multifaceted nature of privacy violations and the importance of robust privacy protections and responsible data handling practices.

E. Cases and Incidents

The following are some instances of empirical cases and incidents that took place in the real world that highlight the practical ramifications of privacy laws and principles:

The 2013 Target data breach (16), which impacted up to 70 million customers, highlighted failures in protecting personal financial information. Despite having data encryption and security protocols, Target lacked robust access controls, allowing hackers to access sensitive credit card data undetected for weeks by breaching a third-party HVAC vendor with ties to Target's systems. This exemplified the real-world effects when organizations neglect the privacy principle of access limitation.

The 2018 Exactis (17) data leak underscored risks of excessive data retention failing to meet data minimization standards. Marketing firm Exactis exposed 340 million individual records - including personal emails, phone numbers, and physical addresses. By amassing vast quantities of consumer data without purpose limitations or disposal policies, Exactis created substantial vulnerabilities that could enable identity theft and financial fraud at scale.

The record €746 million GDPR fine (18) against Amazon in 2021 for breaching EU data protection rules highlights growing regulatory crackdowns on privacy non-compliance. Amazon's processing of behavioral user data for targeted advertising violated transparency and valid consent requirements. This landmark penalty signals that authorities are prioritizing enforcement of core privacy principles codified in laws like GDPR on a global level.

As these cases demonstrate, privacy breaches often arise from organizations overlooking foundational data protection principles like data minimization, purpose limitation, or access control. The expanding patchwork of stringent privacy regulations also shows governments are raising the stakes for compliance through hefty fines, given the scale of potential privacy harms.

Understanding these principles and laws is key for pragmatic protection.

F. Technological Aspects of Privacy Protection

Emerging privacy-enhancing technologies offer promising safeguards while still enabling data utility. Solutions like encryption and anonymization employ sophisticated techniques to uphold personal privacy.

Encryption (19) converts data into coded form, scrambling it so only authorized parties can access the original information. When done effectively, strong encryption allows organizations to analyze patterns and glean insights from data at scale without exposing sensitive personal details. State-of-the-art homomorphic encryption even allows certain computations directly on encrypted data. Though encryption has trade-offs like cost and complexity, it represents a privacy-preserving alternative to cleartext data warehousing.

Anonymization (20) transforms personal data by removing or obscuring identifiers connected to individuals. This curtails the privacy risks of sharing datasets by making re-identification difficult. Methods like generalization and perturbation protect sensitive attributes yet preserve analytical utility. However, complete anonymization without losing too much value remains an active challenge, as unique combinations of less sensitive data can still enable re-identification.

Additionally, multi-party computation distributes data processing across entities so no one party sees full raw datasets. Other emerging controls include granular access policies enforced by blockchain-based identity management and hardware-based trusted execution environments.

Overall, technologies like encryption and anonymization highlight promising paths to balance data use for innovation against individual privacy rights. While technical solutions have limitations, in combination with strong policies and vigilant data governance, privacy-enhancing technologies offer a route towards ethical data systems where vulnerabilities are proactively

minimized by design. Further interdisciplinary collaboration is unlocking cutting-edge controls to make this vision a reality.

III. CONCLUSION

In an era characterized by unprecedented digital connectivity, the concept of privacy has undergone a profound transformation, evolving from a fundamental human right into a complex and multifaceted challenge. Technology, while enabling the seamless exchange of information, has simultaneously given rise to pressing concerns regarding the safeguarding of personal data. As this paper has explored, the core principles of privacy, ranging from data minimization to consent and control, constitute the bedrock of responsible data handling in our interconnected world.

The balance between protecting individuals' privacy rights and fostering innovation in a data-driven society remains a paramount challenge. Striking this balance necessitates collaborative efforts among organizations, policymakers, and technologists to develop privacy-enhancing technologies that promote responsible innovation.

It is important to understand and recognize the various typologies of privacy harms. Understanding the diverse ways in which privacy violations can manifest, from physical and economic to reputational and psychological harms, underscores the urgency of robust privacy protections. The responsibility falls upon individuals, organizations, and governments to ensure that privacy remains a fundamental right, even in our ever-evolving digital landscape. Only by adhering to ethical principles and stringent privacy laws can we continue to navigate this landscape with the assurance that personal data is treated with the respect and protection it deserves.

REFERENCES

- [1] Article 5 of the GDPR. Retrieved September 7, 2023, from <https://gdpr-info.eu/art-5-gdpr/>
- [2] California Consumer Privacy Act. Retrieved September 6, 2023,

- https://cpa.ca.gov/regulations/pdf/cpa_a_ct.pdf
- [3] Scholz, Lauren H. (2019) "Privacy Remedies," *Indiana Law Journal*: Vol. 94: Iss. 2, Article 7. Retrieved September 7, 2023, from: <https://www.repository.law.indiana.edu/ilj/vol94/iss2/7>
- [4] Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477. <https://doi.org/10.2307/40041279>
- [5] Principles of Data Protection | Data Protection Commissioner, <https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection>
- [6] Scholz, Lauren H. (2019) "Privacy Remedies," *Indiana Law Journal*: Vol. 94: Iss. 2, Article 7. Retrieved September 7, 2023, from: <https://www.repository.law.indiana.edu/ilj/vol94/iss2/7>
- [7] Nations, U. (1948, December 10). Universal Declaration of Human Rights. United Nations; United Nations, from <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
- [8] Mixson, E. (2021, June 30). The Pros and Cons of Privacy-Enhancing Technologies (PETs). Cyber Security Hub, from <https://www.cshub.com/executive-decisions/articles/the-pros-and-cons-of-privacy-enhancing-technologies-pets>
- [9] Clarke, R., 2009. Privacy impact assessment: Its origins and development. *Computer Law & Security Review* 25, 123–135.. , from <https://doi.org/10.1016/j.clsr.2009.02.002>
- [10] Harper, J. 17 (2020). Privacy and the Four Categories of Information Technology. American Enterprise Institute, Retrieved September 10, 2023, from <https://www.aei.org/wp-content/uploads/2020/05/Privacy-and-the-Four-Categories-of-Information-Technology.pdf?x91208>

- [11] Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119-157. Retrieved September 10, 2023, from <https://crypto.stanford.edu/portia/papers/RvnissenbaumDTP31.pdf>
- [12] Citron, Danielle Keats and Solove, Daniel J., Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 *Boston University Law Review* 793 (2022). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222
- [13] Canada, O. of the P. C. of. (2021, December 8). The Personal Information Protection and Electronic Documents Act (PIPEDA). <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>
- [14] Personal Data Protection Act 2012—Singapore Statutes Online. (2012). Retrieved September 7, 2023, from <https://sso.agc.gov.sg:5443/Act/PDPA2012>
- [15] Statutes of the Republic of Korea. (2014). Retrieved September 7, 2023, from https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG
- [16] Plachkinova, M., & Maurer, C. (2018). Security breach at target. *Journal of Information Systems Education*, 29(1), 11-20. From <https://aisel.aisnet.org/jise/vol29/iss1/7/>
- [17] Greenberg, A. (2018, June 27). Marketing Firm Exactis Leaked a Personal Info Database With 340 Million Records | WIRED. <https://www.wired.com/story/exactis-database-leak-340-million-records/>
- [18] Hodge, N. (2022, July 29). One year later, Amazon GDPR fine details remain clouded. *Compliance Week | Regulatory Enforcement*, from <https://www.complianceweek.com/regulatory-enforcement/one-year-later-amazon-gdpr-fine-details-remain-clouded/31913.article>
- [19] Jain, P. (2021, July 15). Encryption: A Tradeoff Between User Privacy and National Security. *American University | Technology*, from <https://www.american.edu/sis/centers/security-technology/encryption.cfm>
- [20] Jain, P., Gyanchandani, M. & Khare, N. Big data privacy: a technological perspective and review. *J Big Data* 3, 25 (2016), from <https://doi.org/10.1186/s40537-016-0059-y>