Too long, didn't read

Since the adoption of the General Data Protection Regulation (GDPR) on May 24, 2016, European data privacy legislation has undergone a paradigm shift from being complicated and region-specific to just universally complicated [1]. As GDPR asserts governance over personal data processing in the European Union (EU) and EU data subjects[2]. These legislative changes have impacted the global data privacy landscape and technology development across public and private sectors[3], [4].
Degeling et al. [1] evaluate the impact of GDPR on general web privacy by providing compliance focussed analyses of privacy policies and cookie consent notices from 6759 websites. Though the empirical study presents findings which indicate a positive impact of GDPR on global data privacy, the authors briefly acknowledge potential negative impacts due to the increased cognitive burden on data subjects[1], [5].

We value your privacy:

The authors observed overall improvements to website privacy policies due to GDPR compliance requirements[1].
Though theoretically sound, the idea that data subjects are benefitting from these verbose legal documents in practical ways seems a little closer to fiction. Users are likely to ignore[6] privacy policies due to their terse and time-consuming nature[1], [5], [7].

What is the value of a privacy policy?

Have some cookies

A cookie is "a way for an origin server to send state information to a user agent and for the user agent to return the state information to the origin server" [8].
Primarily, GDPR cookie compliance manifests as cookie consent notices although their implementation is not legally required[2], [5]. Degeling et al. noted the increased sophistication and prevalence of cookie banners around the period of May 2018, when GDPR became legally applicable. This indicates that the burden and level of complexity surrounding GDPR compliance[4] is simply transferred by companies onto users[7], [9]–[11].

"I agree…"

Since GDPR adoption in 2018, several non-EU countries have passed similar data privacy legislation[12], [13]. Although such legislation is generally considered a move in the right direction, their practical implications present more complex issues.
In essence, consent is central to relationships between data subjects and web services, and legislation compliance[1], [2], [5], [9], [10], [14]. Unfortunately, this raises some complex issues around ambiguous interpretations of the terms "informed consent" or "freely given consent".
Is it fair to assume a that a user has provided consent by accepting privacy and cookie policies that are beyond the user's understanding?
Is the consent of children under 16 years of age considered valid without parental guidance or approval?

Can consent be considered valid if it is obtained through an ultimatum which offers no alternatives other than exclusion from or termination of service?

Why should we care?

Would you be comfortable with sharing your internet habits and behaviour anonymously?
Researchers have demonstrated the ability to re-identify 99.98% users from anonymised datasets using only 15 demographic attributes[15].

Who owns the data you provide to a web service?

References

[1] M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz, "We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy," Aug. 2018, doi: 10.14722/ndss.2019.23378.

[2] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. European Union, 2016.

[3] C. Ingley and P. Wells, "GDPR: Governance Implications for Regimes outside the EU."

[4] H. Li, L. Yu, and W. He, "The Impact of GDPR on Global Technology Development," *Journal of Global Information Technology Management*, vol. 22, no. 1. Taylor and Francis Inc., pp. 1–6, Jan. 02, 2019, doi: 10.1080/1097198X.2019.1569186.

[5] S. (Financial executive) Sharma, *Data privacy and GDPR handbook*. .

[6] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services," *Information, Communication & Society*, vol. 23, no. 1, pp. 128–147, 2020.

[7] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies," *Isjlp*, vol. 4, p. 543, 2008.

[8] E. A. Greenberg, "What are cookies?"

[9] R. Slattery and M. Krawitz, "MARK ZUCKERBERG, THE COOKIE MONSTER-AUSTRALIAN PRIVACY LAW AND INTERNET COOKIES." [Online]. Available: www.facebook.com/help/210644045634222.

[10] J. Pierson and R. Heyman, "Social media and cookies: Challenges for online privacy," *Info*, vol. 13, no. 6, pp. 30–42, Sep. 2011, doi: 10.1108/14636691111174243.

[11] A. M. Hormozi, "Cookies and Privacy," *EDPACS*, vol. 32, no. 9, pp. 1–13, Mar. 2005, doi: 10.1201/1079/45030.32.9.20050301/86855.1.

[12] G. Greenleaf, "Global Data Privacy Laws 2019: New Eras for International Standards," 2019.

[13] *Privacy Act 2020*. Wellington: New Zealand Ministry of Justicy, 2020.

[14] B. Goodman and S. Flaxman, "European union regulations on algorithmic decision making and a 'right to explanation,'" *AI Magazine*, vol. 38, no. 3, pp. 50–57, Sep. 2017, doi: 10.1609/aimag.v38i3.2741.

[15] L. Rocher, J. M. Hendrickx, and Y. A. de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," *Nature Communications*, vol. 10, no. 1, Dec. 2019, doi: 10.1038/s41467-019-10933-3.